Chapter 6

Cardinal Numbers

6.1 INTRODUCTION

It is natural to ask whether or not two sets have the same number of elements. For finite sets the answer can be found by simply counting the number of elements. For example, each of the sets

$$\{a,b,c,d\}, \qquad \{2,3,5,7\}, \qquad \{x,y,z,t\}$$

has four elements. Thus these sets have the same number of elements. However, it is not always necessary to know the number of elements in two finite sets before we know that they have the same number of elements. For example, if each chair in a room is occupied by exactly one person and there is no one standing, then clearly there are "just as many" people as there are chairs in the room.

The above simple notion, that two sets have "the same number of elements" if their elements can be "paired-off", can also apply to infinite sets. In fact, it has the following startling results:

(*a*) Infinite sets need not have the "same number of elements"; some are "more infinite" than others.
(*b*) There are "just as many" even integers as there are integers, and "just as many" rational numbers **Q** as positive integers **P**.
(*c*) There are "more" points on the real line **R** than there are positive integers **P**; and there are "more" curves in the plane $\mathbf{R}^2$ than there are points in the plane.

This chapter will investigate and prove the above results. First we will formally define when two sets, finite or infinite, have the same number of elements or, in other words, the same cardinality. Lastly, we define addition and multiplication for these "cardinal numbers", and show that many of their properties reflect corresponding properties of sets.

We remark that, at one time, all infinite sets were considered to have the same number of elements. The German mathematician Georg Cantor (1845–1918) gave the above alternative definition which revolutionized the entire theory of sets.

6.2 ONE-TO-ONE CORRESPONDENCE, EQUIPOTENT SETS

Recall that a one-to-one correspondence between sets A and B is a function $f: A \to B$ which is bijective, that is, which is one-to-one and onto. In such a case, each element $a \in A$ is paired with a unique element $b \in B$ given by $b = f(a)$. We sometimes write

$$a \leftrightarrow b$$

to denote such a pairing.

Remark: Frequently, a child counts the objects of a set by forming a one-to-one correspondence between the objects and his fingers. An adult counts the objects of a set by forming a one-to-one correspondence between the objects and the set

$$\{1,2,3,\ldots,n\}$$

In fact, if one is asked the question:

"How many days are there until next Saturday?"

the response is often to actually pair the remaining days with one's fingers.

The following definition applies.

Definition 6.1: Sets A and B are said to have the *same cardinality* or the *same number of elements*, or to be *equipotent*, written

$$A \approx B$$

if there is a function $f: A \to B$ which is bijective, that is, both one-to-one and onto.

Recall that such a function f is said to define a *one-to-one correspondence* between A and B.

Since the identity function is bijective, and the composition and inverse of bijective functions are bijective, we immediately obtain the following theorem:

Theorem 6.1: The relation $\approx$ of being equipotent is an equivalence relation in any collection of sets. That is:

(i) $A \approx A$ for any set A.

(ii) If $A \approx B$, then $B \approx A$.

(iii) If $A \approx B$ and $B \approx C$, then $A \approx C$.

EXAMPLE 6.1

(*a*) Let A and B be sets with exactly three elements, say,

$$A = \{2, 3, 5\}, \quad \text{and } B = \{\text{Marc, Erik, Audrey}\}$$

Then clearly we can find a one-to-one correspondence between A and B. For example, we can label the elements of A as the first element, the second element, and the third element, and label B similarly. Then the rule which pairs the first elements of A and B, pairs the second elements of A and B, and pairs the third elements of A and B, that is, the function $f: A \to B$ defined by

$$f(2) = \text{Marc}, \quad f(3) = \text{Erik}, \quad f(5) = \text{Audrey}$$

is one-to-one and onto. Thus A and B are equipotent.

The same idea may be used to show that any two finite sets with the same number of elements are equipotent.

(*b*) Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$. Then A and B are not equipotent. For suppose there were a rule for pairing the elements of A and B. If there were four or more pairs, then an element of B would be used twice, and if there were three or fewer pairs then some element of A would not be used. In other words, since A has more elements than B, any function $f: A \to B$ must assign at least two elements of A to the same element of B, and hence f would not be one-to-one.

In a similar way, we can see that any two finite sets with different numbers of elements are not equipotent.

(*c*) Let $\mathbf{I} = [0, 1]$, the closed unit interval, and let S be any other closed interval, say $S = [a, b]$ where $a < b$. The function $f: \mathbf{I} \to S$ defined by

$$f(x) = (b - a)x + a$$

is one-to-one and onto. Thus $\mathbf{I}$ and S have the same cardinality. Therefore, by Theorem 6.1, any two closed intervals have the same cardinality.

(*d*) Consider the set $\mathbf{P} = \{1, 2, 3, \ldots\}$ of positive integers and the set $E = \{2, 4, 6, \ldots\}$ of even positive integers. The following defines a one-to-one correspondence between $\mathbf{P}$ and E:

$$\begin{array}{rccccccccc} \mathbf{P} = \{1, & 2, & 3, & 4, & 5, & . & . & .\} \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ E = \{2, & 4, & 6, & 8, & 10, & . & . & .\} \end{array}$$

In other words, the function $f: \mathbf{P} \to E$ defined by $f(n) = 2n$ is one-to-one and onto. Thus $\mathbf{P}$ and E have the same cardinality.

More generally, if $K = \{0, k, 2k, 3k, \ldots\}$ is the set of multiples of a positive integer k, then $f: \mathbf{P} \to K$ defined by $f(n) = kn$ is a one-to-one correspondence between $\mathbf{P}$ and K. Therefore $\mathbf{P}$ and K have the same cardinality.

Parts (a) and (b) of the above Example 6.1 show that finite sets are equipotent if and only if they contain the same number of elements. Thus, for finite sets, Definition 6.1 corresponds to the usual meaning of two sets containing the same number of elements.

On the other hand, Example 6.1(d) shows that the infinite set $\mathbf{P}$ has the same cardinality as a proper subset of itself. This property is characteristic of infinite sets. In fact, we state this observation formally.

Definition 6.2: A set S is *infinite* if it has the same cardinality as a proper subset of itself. Otherwise S is *finite*.

Familiar examples of infinite sets are the counting numbers (positive integers) $\mathbf{P}$, the natural numbers (nonnegative integers) $\mathbf{N}$, the integers $\mathbf{Z}$, the rational numbers $\mathbf{Q}$, and the real numbers $\mathbf{R}$.

There might be a temptation to think that all infinite sets have the same cardinality; but we will show later that this is definitely not true.

We conclude this section with the following example, which tells us that any two sets have the same cardinality, respectively, to two disjoint sets.

EXAMPLE 6.2 Consider any two sets A and B. Let $A' = A \times \{1\}$ and $B' = B \times \{2\}$. Then

$$A \approx A' \quad \text{and} \quad B \approx B'$$

For example, the functions

$$f(a) = (a, 1),\ a \in A \quad \text{and} \quad g(b) = (b, 2),\ b \in B$$

are each bijective. Although A and B need not be disjoint, the sets A' and B' are disjoint, i.e.,

$$A' \cap B' = \varnothing$$

Specifically, each ordered pair in A' has 1 as a second component, whereas each ordered pair in B' has 2 as a second component.

6.3 DENUMERABLE AND COUNTABLE SETS

The reader is familiar with the set $\mathbf{P} = \{1, 2, 3, \ldots\}$ of counting numbers or positive integers. The following definitions apply.

Definition 6.3: A set D is said to be *denumerable* or *countably infinite* if D has the same cardinality as $\mathbf{P}$.

Definition 6.4: A set is *countable* if it is finite or denumerable, and a set is *nondenumerable* if it is not countable.

Thus a set S is nondenumerable if S is infinite and S does not have the same cardinality as $\mathbf{P}$.

EXAMPLE 6.3

(a) Any infinite sequence

$$a_1, a_2, a_3, \ldots$$

of distinct elements is countably infinite, for a sequence is essentially a function $f(n) = a_n$ whose domain is $\mathbf{P}$. So if the a_n are distinct, the function is one-to-one and onto. Thus each of the following sets is countably infinite:

$$\{1, 1/2, 1/3, \ldots, 1/n, \ldots\}$$
$$\{1, -2, 3, -4, \ldots (-1)^{n-1} n, \ldots\}$$
$$\{(1, 1), (4, 8), (9, 27), \ldots, (n^2, n^3), \ldots\}$$

(*b*) Consider the product set $\mathbf{P} \times \mathbf{P}$ as exhibited in Fig. 6-1. The set $\mathbf{P} \times \mathbf{P}$ can be written as an infinite sequence as follows:

$$\{(1,1),\ (2,1),\ (1,2),\ (1,3),\ (2,2),\ldots\}$$

This sequence is determined by "following the arrows" in Fig. 6-1. Thus $\mathbf{P} \times \mathbf{P}$ is countably infinite for the reasons stated in (*a*).

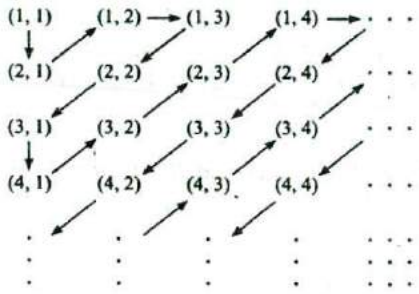


Fig. 6-1

(*c*) Recall that $\mathbf{N} = \{0, 1, 2, \ldots\} = \mathbf{P} \cup \{0\}$ is the set of natural numbers or nonnegative integers. Now each positive integer $a \in \mathbf{P}$ can be written uniquely in the form

$$a = 2^r(2s + 1)$$

where $r, s \in \mathbf{N}$. Consider the function f: $\mathbf{P} \to \mathbf{N} \times \mathbf{N}$ defined by

$$f(a) = (r, s)$$

where r and s are as above. Then f is one-to-one and onto. Thus $\mathbf{N} \times \mathbf{N}$ is denumerable (countably infinite) or, in other words, $\mathbf{N} \times \mathbf{N}$ has the same cardinality as $\mathbf{P}$. Note that $\mathbf{P} \times \mathbf{P}$ is a subset of $\mathbf{N} \times \mathbf{N}$.

The following theorems apply.

Theorem 6.2: Every infinite set contains a subset which is denumerable.

Theorem 6.3: A subset of a denumerable set is finite or denumerable.

Corollary 6.4: A subset of a countable set is countable.

Theorem 6.5: Let $A_1, A_2, A_3, \ldots$ be a sequence of pairwise disjoint denumerable sets. Then the union

$$A_1 \cup A_2 \cup A_3 \cup \cdots = \cup\{A_i : i \in \mathbf{P}\}$$

is denumerable.

Corollary 6.6: A countable union of countable sets is countable.

Observe that Corollary 6.6 tells us that if each of the sets $A_1, A_2, A_3, \ldots$ is countable then the union

$$A_1 \cup A_2 \cup A_3 \cup \cdots$$

is also countable.

The next theorem gives a very important, and not entirely obvious, example of a denumerable (countably infinite) set.

Theorem 6.7: The set $\mathbf{Q}$ of rational numbers is denumerable.

Proof: Note that $\mathbf{Q} = \mathbf{Q}^+ \cup \{0\} \cup \mathbf{Q}^-$ where $\mathbf{Q}^+$ and $\mathbf{Q}^-$ denote, respectively, the sets of positive and negative rational numbers. Let $f: \mathbf{Q}^+ \to \mathbf{P} \times \mathbf{P}$ be defined by

$$f(p/q) = (p, q)$$

where p/q is any element of $\mathbf{Q}^+$ expressed as the ratio of two relatively prime positive integers. Then f is one-to-one and so $\mathbf{Q}^+$ has the same cardinality as a subset of $\mathbf{P} \times \mathbf{P}$. By Example 6.3($b$), $\mathbf{P} \times \mathbf{P}$ is denumerable; hence, by Theorem 6.3, the infinite set $\mathbf{Q}^+$ is denumerable. Similarly $\mathbf{Q}^-$ is denumerable. Thus the set $\mathbf{Q}$ of rational numbers, the union of $\mathbf{Q}^+$, $\{0\}$, and $\mathbf{Q}^-$, is also denumerable.

Remark: Theorem 6.7 tells us that there are just as many rational numbers as there are positive integers, that is, that $\mathbf{Q}$ has the same cardinality as $\mathbf{P}$.

6.4 REAL NUMBERS R AND THE POWER OF THE CONTINUUM

Not every infinite set is countable. The next theorem (proved in Problem 6.15) gives a specific and extremely important example of such a set.

Theorem 6.8: The unit interval $\mathbf{I} = [0, 1]$ is nondenumerable.

Observe that this theorem also tells us that infinite sets need not have the same cardinality.

The following definition applies.

Definition 6.5: A set A is said to have the *power of the continuum* if A has the same cardinality as the unit interval $\mathbf{I} = [0, 1]$.

Besides the unit interval $\mathbf{I}$, all the other intervals also have the power of the continuum. There are several such kinds of intervals. Specifically, if a and b are real numbers with $a < b$, then we define:

closed interval:	$[a, b] = \{x \in \mathbf{R} : a \leq x \leq b\}$
open interval:	$(a, b) = \{x \in \mathbf{R} : a < x < b\}$
half-open intervals:	$[a, b) = \{x \in \mathbf{R} : a \leq x < b\}$
	$(a, b] = \{x \in \mathbf{R} : a < x \leq b\}$

Example 6.1(c) shows that any closed interval $[a, b]$ has the power of the continuum. Problem 6.3 shows that any open or half-open interval also has the power of the continuum.

Real Numbers R

Lastly, we note that the set $\mathbf{R}$ of real numbers also has the power of the continuum. Specifically, consider the function $f: \mathbf{R} \to D$ where $D = (-1, 1)$ and f is defined by

$$f(x) = \frac{x}{1 + |x|}$$

Figure 6-2 is the graph of this function. Clearly the values of f belong to $(-1, 1)$ since $|x| < 1 + |x|$. It is not difficult to show that f is both one-to-one and onto. Thus the set $\mathbf{R}$ of real numbers has the same cardinality as the open interval $D = (-1, 1)$, and hence $\mathbf{R}$ has the power of the continuum.

Remark: Some texts define a set A to have the power of the continuum if it has the same cardinality as $\mathbf{R}$ rather than the unit interval $\mathbf{I}$. By the above remark, both definitions are equivalent. The use here of $\mathbf{I}$ rather than $\mathbf{R}$ is motivated by Theorem 6.8.

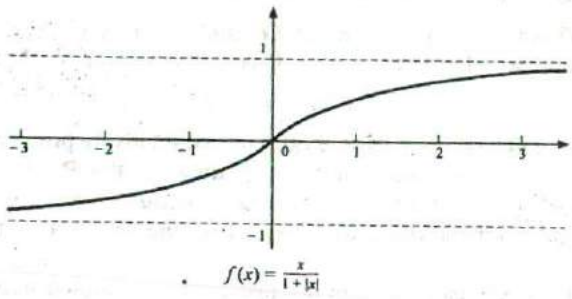


Fig. 6-2

6.5 CARDINAL NUMBERS

Frequently, we want to know the "size" of a given set without necessarily comparing it to another set. For finite sets, there is no difficulty. For example, the set $A = \{a, b, c\}$ has 3 elements. Any other set with 3 elements is equipotent to A. On the other hand, for infinite sets it is not sufficient to just say that the set has infinitely many elements since not all infinite sets are equipotent. To solve this problem, we introduce the concept of a cardinal number.

Each set A is assigned a symbol in such a way that two sets A and B are assigned the same symbol if and only if they are equipotent. This symbol is called the *cardinality* or *cardinal number* of A, and it is denoted by

$$|A|, \quad n(A), \quad \text{or} \quad \text{card}(A)$$

We will use $|A|$. Thus:

$$\boxed{|A| = |B| \quad \text{if and only if} \quad A \approx B}$$

One may also view a cardinal number as the equivalence class of all sets which are equipotent.

Finite Cardinal Numbers

The obvious symbols are used for the cardinal numbers of finite sets. That is, 0 is assigned to the empty set $\varnothing$, and n is assigned to the set $\{1, 2, \ldots, n\}$. Thus:

$$\boxed{|A| = n \quad \text{if and only if} \quad A \approx \{1, 2, \ldots, n\}}$$

Alternatively, the symbols $0, 1, 2, 3, \ldots$ are assigned, respectively, to the sets

$$\varnothing, \{\varnothing\}, [\varnothing, \{\varnothing\}], [\varnothing, \{\varnothing\}, [\varnothing, \{\varnothing\}]], \ldots$$

Although the natural number n and the cardinal number n are technically different things, there is no conflict using the same symbol in these two roles. The cardinal numbers of finite sets are called *finite cardinal numbers*.

Transfinite Cardinal Numbers, $\aleph_0$ and $\mathbf{c}$

Cardinal numbers of infinite sets are called *infinite* or *transfinite cardinal numbers*. The cardinal number of the infinite set $\mathbf{P}$ of positive integers is

$$\aleph_0$$

which is read aleph-nought. This notation was introduced by Cantor. (The symbol $\aleph$ is the first letter aleph of the Hebrew alphabet.) Thus:

$$|A| = \aleph_0 \quad \text{if and only if} \quad A \approx \mathbf{P}$$

In particular, we have $|\mathbf{Z}| = \aleph_0$ and $|\mathbf{Q}| = \aleph_0$. (The significance of 0 in $\aleph_0$ is discussed in Chapter 8.)

The cardinal number of the unit interval $\mathbf{I} = [0, 1]$ is denoted by:

$$\mathbf{c}$$

and it is called the *power of the continuum*. Thus:

$$|A| = \mathbf{c} \quad \text{if and only if} \quad A \approx \mathbf{I}$$

In particular, we have $|\mathbf{R}| = \mathbf{c}$, and the cardinal number of any interval is $\mathbf{c}$.

The following statements follow directly from the above definitions:

(*a*) A is denumerable or countably infinite means $|A| = \aleph_0$.
(*b*) A is countable means $|A|$ is finite or $|A| = \aleph_0$.
(*c*) A has the power of the continuum means $|A| = \mathbf{c}$.

6.6 ORDERING OF CARDINAL NUMBERS

One frequently wants to compare the size of two sets. This is done by means of an inequality relation which is defined for cardinal numbers as follows.

Definition 6.6: Let A and B be sets. We say that

$$|A| \leq |B|$$

if A has the same cardinality as a subset of B or, equivalently, if there exists a one-to-one (injective) function $f: A \to B$.

As expected, $|A| \leq |B|$ is read:

"The cardinal number of A is less than or equal to the cardinal number of B."

As usual with the symbol $\leq$, we have the following addition notation:

$$\begin{array}{lll} |A| < |B| & \text{means} & |A| \leq |B| \quad \text{but } |A| \neq |B| \\ |A| \geq |B| & \text{means} & |B| \leq |A| \\ |A| > |B| & \text{means} & |B| < |A| \end{array}$$

Again, as usual, the symbols $<$, $\geq$, $>$ are read "less than", "greater than or equal to", and "greater than", respectively.

We emphasize that the above relations between cardinal numbers are well defined, that is, the relations are independent of the particular sets involved. Namely, if $A \approx A'$ and $B \approx B'$, then

$$|A| \leq |B| \text{ if and only if } |A'| \leq |B'| \quad \text{and} \quad |A| < |B| \text{ if and only if } |A'| < |B'|$$

EXAMPLE 6.4

(*a*) Let A be a proper subset of a finite set B. Clearly, $|A| \leq |B|$. Since A is a proper subset of B, where A and B are finite, we know that $|A| \neq |B|$. Thus $|A| < |B|$. In other words, for finite cardinals m and n, we have $m < n$ as cardinal numbers if and only if $m < n$ as nonnegative integers. Accordingly, the inequality relation $\leq$ for cardinal numbers is an extension of the inequality relation $\leq$ for nonnegative integers.

(*b*) Let n be a finite cardinal. Then $n < \aleph_0$ since any finite set A is equipotent to a subset of $\mathbf{P}$ and $|A| \neq |\mathbf{P}|$. Thus we may write

$$0 < 1 < 2 < \cdots < \aleph_0$$

(*c*) Consider the set $\mathbf{P}$ of positive integers and the unit interval $\mathbf{I}$, that is, consider the sets

$$\mathbf{P} = \{1, 2, 3, \ldots\} \quad \text{and} \quad \mathbf{I} = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$$

The function $f: \mathbf{P} \to \mathbf{I}$ defined by $f(n) = 1/n$ is one-to-one. Therefore, $|\mathbf{P}| \leq |\mathbf{I}|$. On the other hand, by Theorem 6.7, $|\mathbf{P}| \neq |\mathbf{I}|$. Therefore, $\aleph_0 = |\mathbf{P}| < |\mathbf{I}| = \mathfrak{c}$. Accordingly, we may now write

$$0 < 1 < 2 < \cdots < \aleph_0 < \mathfrak{c}$$

(*d*) Let A be any infinite set. By Theorem 6.2, A contains a subset which is denumerable. Accordingly, for any infinite set A, we always have $\aleph_0 \leq |A|$.

Cantor's Theorem

The only transfinite cardinal numbers we have seen are $\aleph_0$ and $\mathfrak{c}$. It is natural to ask if there are any others. The answer is yes. In fact, Cantor's theorem, which follows, tells us that the cardinal number of the power set $\mathscr{P}(A)$ of any set A is larger than the cardinal number of the set A itself; namely:

Theorem 6.9 (Cantor): For any set A, we have $|A| < |\mathscr{P}(A)|$.

This important theorem is proved in Problem 6.18.

Notation: If $\alpha = |A|$, then we let $2^{\alpha} = |\mathscr{P}(A)|$. This no doubt comes from the fact that if a finite set A has n elements then $\mathscr{P}(A)$ has 2^n elements.

Accordingly, Cantor's theorem may be restated as follows.

Theorem 6.9 (Cantor): For any cardinal number α, we have $\alpha < 2^{\alpha}$.

Schroeder–Bernstein Theorem, Law of Trichotomy

Note first that the relation $\leq$ for cardinal numbers is reflexive and transitive. That is:

(i) For any set A, we have $|A| = |A|$.

(ii) If $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

The second property (transitivity) comes from the fact that if $f: A \to B$ and $g: B \to C$ are both one-to-one, then the composition $g \circ f: A \to C$ is also one-to-one.

Since we have used the familiar $\leq$ notation, we would hope that the relation $\leq$ for cardinal numbers possesses other commonly used properties of the relation $\leq$ for the real numbers $\mathbf{R}$ and the integers $\mathbf{Z}$. One such property follows:

> If a and b are real numbers such that $a \leq b$ and $b \leq a$, then $a = b$.

This property certainly holds for finite cardinal numbers. If A is a proper subset of a finite set B, then $|A| < |B|$. Therefore, for finite sets A and B, the only way that we can have $|A| \leq |B|$ and $|B \leq |A|$ is that A and B have the same number of elements, that is, that $|A| = |B|$.

On the other hand, it is possible for a proper subset of an infinite set to have as many elements as the entire set. For example, consider the infinite sets

$$E = \{2, 4, 6, \ldots\} \qquad \text{and} \qquad \mathbf{P} = \{1, 2, 3, \ldots\}$$

As illustrated in Example 6.1(d), the subset E does have the same cardinality as $\mathbf{P}$. Accordingly, the above property for infinite cardinal numbers is not obvious. But it is still indeed true in view of the celebrated Schroeder–Bernstein theorem which follows.

Theorem 6.10 (Schroeder–Bernstein): If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

In other words, if α and β are cardinal numbers such that $\alpha \leq \beta$ and $\beta \leq \alpha$, then $\alpha = \beta$. This important theorem, proved in Problem 6.19, can be stated in the following equivalent form.

Theorem 6.11: Let X, Y, X_1 be sets such that $X \supseteq Y \supseteq X_1$ and $X \approx X_1$. Then $X \approx Y$.

Another familiar property of the relation $\leq$ for the real numbers $\mathbf{R}$, called the law of trichotomy, is the following:

> If a and b are real numbers, then exactly one of the following is true:
> $$a < b, \qquad a = b, \qquad a > b$$

It is clear that the above property holds for finite cardinal numbers. Again, it is not obvious that it holds for infinite cardinal numbers. The fact that it does is the content of the next theorem.

Theorem 6.12 (Law of Trichotomy): For any two sets A and B, exactly one of the following is true:

$$|A| < |B|, \qquad |A| = |B|, \qquad |A| > |B|$$

In other words, if α and β are cardinal numbers, then either $\alpha < \beta$, $\alpha = \beta$, or $\alpha > \beta$. The proof of this theorem uses transfinite induction which is discussed in Chapter 9; hence the proof will be postponed until then.

Continuum Hypothesis

By Cantor's theorem, $\aleph_0 < 2^{\aleph_0}$ and, as noted previously, $\aleph_0 < \mathbf{c}$. The next theorem (proved in Problem 6.20) tells us the relationship between $2^{\aleph_0}$ and $\mathbf{c}$.

Theorem 6.13: $2^{\aleph_0} = \mathbf{c}$.

It is natural to ask if there exists a cardinal number β which lies "between" $\aleph_0$ and $\mathbf{c}$. Originally, Cantor supported the conjecture, which is known as the continuum hypothesis, that the answer to the above question is in the negative. Specifically:

Continuum Hypothesis: There exists no cardinal number β such that

$$\aleph_0 < \beta < \mathbf{c}$$

In 1963 it was shown by Paul Cohen that the continuum hypothesis is independent of our axioms of set theory in somewhat the same sense that Euclid's fifth postulate on parallel lines is independent of the other axioms of geometry.

6.7 CARDINAL ARITHMETIC

The collection of all cardinal numbers can be considered to be a superset of the finite cardinal numbers (nonnegative integers)

$$0, 1, 2, 3, \ldots$$

This section shows how certain arithmetic operations on the finite cardinals can be extended to all the cardinal numbers.

Cardinal Addition and Multiplication

Addition and multiplication of the counting numbers **N** are sometimes treated from the point of view of set theory. The interpretation of $2 + 3 = 5$, for example, is given by the picture in Fig. 6-3. Namely, the union of two disjoint sets, one having two elements and the other having three elements, is a set with five elements. This idea leads to a completely general definition of addition of cardinal numbers.

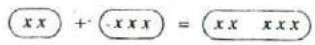


Fig. 6-3

Definition 6.7: Let α and β be cardinal numbers and let A and B be disjoint sets with $\alpha = |A|$ and $\beta = |B|$. Then the *sum* of α and β is denoted and defined by

$$\alpha + \beta = |(A \cup B)|$$

Two comments are appropriate with this definition. First of all, the addition of cardinal numbers is well-defined. That is, if A' and B' are also disjoint sets with cardinality α and β respectively, then

$$|(A' \cup B')| = |(A \cup B)|$$

Second, if A and B are any two sets, then $A \times \{1\}$ and $B \times \{2\}$ are disjoint. Accordingly, there is no difficulty in finding disjoint sets with given cardinalities.

EXAMPLE 6.5

(*a*) Let m and n be finite cardinal numbers. Then $m + n$ corresponds to the usual addition in **N**.

(*b*) Let n be a finite cardinal number. Then $n + \aleph_0 = \aleph_0$ since

$$n + \aleph_0 = |\{1, 2, \ldots, n\} \cup \{n + 1, n + 2, \ldots\}| = \aleph_0$$

(*c*) $\aleph_0 + \aleph_0 = \aleph_0$ since

$$\aleph_0 + \aleph_0 = |\{2, 4, 6, \ldots\} \cup \{1, 3, 5, \ldots\}| = \aleph_0$$

(*d*) $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$ since

$$\mathfrak{c} + \mathfrak{c} = |[0, \tfrac{1}{2}] \cup (\tfrac{1}{2}, 1]| = \mathfrak{c}$$

The definition of cardinal multiplication follows.

Definition 6.8: Let α and β be cardinal numbers and let A and B be sets with $\alpha = |A|$ and $\beta = |B|$. Then the *product* of α and β is denoted and defined by

$$\alpha\beta = |A \times B|$$

As with addition, multiplication of cardinal numbers is well-defined. (Observe that, in the definition of cardinal multiplication, A and B need not be disjoint.)

EXAMPLE 6.6

(*a*) Let m and n be finite cardinal numbers. Then mn corresponds to the usual multiplication in $\mathbf{N}$.

(*b*) Since $\mathbf{N} \times \mathbf{N}$ is countably infinite, $\aleph_0\aleph_0 = \aleph_0$.

(*c*) Theorem 6.15 below tells us that the cartesian plane $\mathbf{R}^2$ has the same cardinality as $\mathbf{R}$. That is, $\mathfrak{c}\mathfrak{c} = \mathfrak{c}$.

Table 6-1 lists properties of the addition and multiplication of cardinal numbers and gives the corresponding properties of sets under union and cartesian product. We state this result formally.

Theorem 6.14: The addition and multiplication of cardinal numbers satisfy the properties in Table 6-1.

Table 6-1

Cardinal numbers	Sets
(1) $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$	(1) $(A \cup B) \cup C = A \cup (B \cup C)$
(2) $\alpha+\beta = \beta+\alpha$	(2) $A \cup B = B \cup A$
(3) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$	(3) $(A \times B) \times C \approx A \times (B \times C)$
(4) $\alpha\beta = \beta\alpha$	(4) $A \times B \approx B \times A$
(5) $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$	(5) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
(6) If $\alpha \le \beta$, then $\alpha+\gamma \le \beta+\gamma$	(6) If $A \subseteq B$, then $(A \cup C) \subseteq (B \cup C)$
(7) If $\alpha \le \beta$, then $\alpha\gamma \le \beta\gamma$	(7) If $A \subseteq B$, then $(A \times C) \subseteq (B \times C)$

We emphasize that not every property of addition and multiplication of finite cardinals holds for cardinal numbers in general. For example, cancellation holds for finite cardinal numbers, that is,

(i) If $a+b = a+c$, then $b = c$.

(ii) If $ab = ac$ and $a \neq 0$, then $b = c$.

On the other hand, using Example 6.5 and Example 6.6, we have

(i) $\aleph_0 + \aleph_0 = \aleph_0 = \aleph_0 + 1$, but $\aleph_0 \neq 1$.

(ii) $\aleph_0\aleph_0 = \aleph_0 = \aleph_0 1$, but $\aleph_0 \neq 1$.

Accordingly, the cancellation law is not true for the operations of addition and multiplication of infinite cardinal numbers.

On the other hand, the addition and multiplication of infinite cardinal numbers turn out to be very simple. We state the following theorem whose proof lies beyond the scope of this text.

Theorem 6.15: Let α and β be nonzero cardinal numbers such that β is infinite and $\alpha \le \beta$. Then

$$\alpha + \beta = \alpha\beta = \beta$$

That is, given two nonzero cardinal numbers, at least one of which is infinite, their sum or product is simply the larger of the two. Examples 6.5 and 6.6 verify some instances of the theorem.

Exponents and Cardinal Numbers

First we note that if A and B are sets, then

$$A^B$$

denotes the set of all functions from B (the exponent) into A. This notation comes from the fact that if A and B are finite sets, say, $|A| = m$ and $|B| = n$, then there are m^n functions from B into A. This is illustrated in the next example, where $|A| = 2$ and $|B| = 3$.

EXAMPLE 6.7 Let $A = \{1, 2\}$ and $B = \{x, y, z\}$. Then A^B consists of exactly eight functions, which follow:

$$\{(x,1),(y,1),(z,1)\}, \quad \{(x,1),(y,1),(z,2)\}, \quad \{(x,1),(y,2),(z,1)\}, \quad \{(x,1),(y,2),(z,2)\},$$
$$\{(x,2),(y,1),(z,1)\}, \quad \{(x,2),(y,1),(z,2)\}, \quad \{(x,2),(y,2),(z,1)\}, \quad \{(x,2),(y,2),(z,2)\}$$

That is, there are 2 choices for x, 2 choices for y, and 2 choices for z, and hence there are $2^3 = 8$ functions altogether.

Exponents are introduced into the arithmetic of cardinal numbers in the next definition and, as illustrated above, this definition agrees with the case when A and B are finite sets.

Definition 6.9: Let α and β be cardinal numbers and let A and B be sets with $\alpha = |A|$ and $\beta = |B|$. Then α *to the power* β is denoted and defined by

$$\alpha^{\beta} = |A^B|$$

Remark: Previously, if $\alpha = |A|$, then we used the exponent notation $2^{\alpha} = |\mathscr{P}(A)|$ where $\mathscr{P}(A)$ is the power set (collection of all subsets) of a set A. We note that there is a one-to-one correspondence between the subsets X of A and functions $f: A \to \{0, 1\}$ as follows:

$$f(a) = \begin{cases} 1 & \text{if } a \in X \\ 0 & \text{if } a \notin X \end{cases}$$

Thus there is no contradiction between the two notations.

The following familiar rules for working with exponents continue to hold.

Theorem 6.16: Let α, β, γ be cardinal numbers. Then:

(1) $(\alpha\beta)^{\gamma} = \alpha^{\gamma}\beta^{\gamma}$. (3) $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\gamma}$.
(2) $\alpha^{\beta}\alpha^{\gamma} = \alpha^{(\beta+\gamma)}$. (4) If $\alpha \le \beta$, then $\alpha^{\gamma} \le \beta^{\gamma}$.

EXAMPLE 6.8 Using the rules for exponentiation, we can make the following calculations:

(*a*) $\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$.

(*b*) $\mathfrak{c}^{\mathfrak{c}} = (2^{\aleph_0})^{\mathfrak{c}} = 2^{\aleph_0 \mathfrak{c}} = 2^{\mathfrak{c}}$.

Solved Problems

EQUIPOTENT SETS, DENUMERABLE SETS, CONTINUUM

6.1. Consider the following concentric circles:

$$C_1 = \{(x, y) : x^2 + y^2 = a^2\}, \qquad C_2 = \{(x, y) : x^2 + y^2 = b^2\}$$

where, say, $0 < a < b$. Establish, geometrically, a one-to-one correspondence between C_1 and C_2.

Let $x \in C_2$. Consider the function $f: C_2 \to C_1$ where $f(x)$ is the point of intersection of the radius from the center of C_2 (and C_1) to x and C_1, as shown in Fig. 6-4. Note that f is both one-to-one and onto. Thus f defines a one-to-one correspondence between C_1 and C_2.

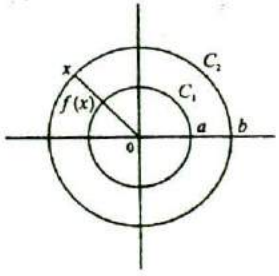


Fig. 6-4

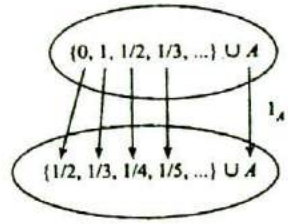


Fig. 6-5

6.2. Prove: (*a*) $[0,1] \approx (0,1)$; (*b*) $[0,1] \approx [0,1)$; (*c*) $[0,1] \approx (0,1]$.

(*a*) Note that

$$[0,1] = \{0, 1, 1/2, 1/3, \ldots\} \cup A$$
$$(0,1) = \{1/2, 1/3, 1/4, \ldots\} \cup A$$

where

$$A = [0,1] \setminus \{0, 1, 1/2, 1/3, \ldots\} = (0,1) \setminus \{1/2, 1/3, \ldots\}$$

Consider the function $f\colon [0,1] \to (0,1)$ defined by the diagram in Fig. 6-5. That is,

$$f(x) = \begin{cases} 1/2 & \text{if } x = 0 \\ 1/(n+2) & \text{if } x = 1/n, n \in \mathbf{P} \\ x & \text{if } x \neq 0, 1/n, n \in \mathbf{P} \end{cases}$$

The function f is one-to-one and onto. Consequently, $[0,1] \approx (0,1)$.

(*b*) The function $f\colon [0,1] \to [0,1)$ defined by

$$f(x) = \begin{cases} 1/(n+1) & \text{if } x = 1/n, n \in \mathbf{P} \\ x & \text{if } x \neq 1/n, n \in \mathbf{P} \end{cases}$$

is one-to-one and onto. [It is similar to the function in part (*a*).] Hence $[0,1] \approx [0,1)$.

(*c*) Let $f\colon [0,1) \to (0,1]$ be the function defined by $f(x) = 1 - x$. Then f is one-to-one and onto and, therefore, $[0,1) \approx (0,1]$. By part (*b*) and Theorem 6.1, we have $[0,1] \approx (0,1]$.

6.3. Prove that each of the following intervals (where $a < b$) has the power of the continuum, i.e., has cardinality **c**:

$$(1)\ [a,b], \qquad (2)\ (a,b), \qquad (3)\ [a,b), \qquad (4)\ (a,b]$$

The formula $f(x) = a + (b-a)x$ defines a bijective mapping between each pair of sets:

(1) $[0,1)$ and $[a,b]$ (3) $[0,1)$ and $[a,b)$
(2) $(0,1)$ and (a,b) (4) $(0,1]$ and $(a,b]$

Thus, by Theorem 6.1 and Problem 6.2, every interval has the same cardinality as the unit interval $\mathbf{I} = [0,1]$, that is, has the power of the continuum.

6.4. Prove Theorem 6.1: The relation $A \approx B$ in sets is an equivalence relation. Specifically:

(1) $A \approx A$ for any set A.

(2) If $A \approx B$, then $B \approx A$.

(3) If $A \approx B$ and $B \approx C$, then $A \approx C$.

(1) The identity function $1_A : A \to A$ is bijective (one-to-one and onto); hence $A \approx A$.

(2) Suppose $A \approx B$. Then there exists a bijective function $f: A \to B$. Hence f has an inverse function $f^{-1}: B \to A$ which is also bijective. Hence $B \approx A$. Therefore, if $A \approx B$ then $B \approx A$.

(3) Suppose $A \approx B$ and $B \approx C$. Then there exist bijective functions $f: A \to B$ and $g: B \to C$. Then the composition function $g \circ f: A \to C$ is also bijective. Hence $A \approx B$. Therefore, if $A \approx B$ and $B \approx C$, then $A \approx C$.

6.5. Prove Theorem 6.2: Every infinite set A contains a subset D which is denumerable.

Let $f: \mathscr{P}(A) \to A$ be a choice function. Consider the following sequence:

$$\begin{aligned} a_1 &= f(A) \\ a_2 &= f(A \backslash \{a_1\}) \\ a_3 &= f(A \backslash \{a_1, a_2\}) \\ &\cdots\cdots\cdots\cdots \\ a_n &= f(A \backslash \{a_1, a_2, \ldots, a_{n-1}\}) \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

Since A is infinite, $A \backslash \{a_1, a_2, \ldots, a_{n-1}\}$ is not empty for every $n \in \mathbf{P}$. Furthermore, since f is a choice function,

$$a_n \neq a_i \qquad \text{for} \qquad i < n$$

Thus the a_n are distinct and, therefore, $D = \{a_1, a_2, \ldots\}$ is a denumerable subset of A.

Essentially, the choice function f "chooses" an element $a_1 \in A$, then chooses an element a_2 from the elements which "remain" in A, and so on. Since A is infinite, the set of elements which "remain" in A is nonempty.

6.6. Prove: (*a*) For any sets A and B, $A \times B \approx B \times A$.

(*b*) For any sets A, B, C,

$$(A \times B) \times C \approx A \times B \times C \approx A \times (B \times C)$$

(*c*) If $A \approx C$ and $B \approx D$, then $A \times B \approx C \times D$.

(*a*) Let $f: A \times B \to B \times A$ be defined by

$$f((a,b)) = (b,a)$$

Clearly f is bijective. Hence $A \times B \approx B \times A$.

(*b*) Let $f: (A \times B) \times C \to A \times B \times C$ be defined by

$$f((a,b),c) = (a,b,c)$$

Then f is bijective. Hence $(A \times B) \times C \approx A \times B \times C$. Similarly, $A \times (B \times C) \approx A \times B \times C$. Thus

$$(A \times B) \times C \approx A \times B \times C \approx A \times (B \times C)$$

(c) Let $f: A \to C$ and $g: B \to D$ be one-to-one correspondences. Define $h: A \times B \to C \times D$ by

$$h(a, b) = (f(a), g(b))$$

One can easily check that h is one-to-one and onto. Hence $A \times B \approx C \times D$.

6.7. Prove: Let X be any set and let $C(X)$ be the family of characteristic functions of X, that is, the family of functions $f: X \to \{0, 1\}$. Then $\mathscr{P}(X) \approx C(X)$ where $\mathscr{P}(X)$ is the power set of X, i.e., the collection of subsets of X.

Let A be any subset of X, i.e., let $A \in \mathscr{P}(X)$. Let $f: \mathscr{P}(X) \to C(X)$ be defined by

$$f(A) = \chi_A$$

that is, f maps each subset A of X into the characteristic function χ_A of A (relative to X). [Recall $\chi_A : X \to \{0, 1\}$ is defined by $f(x) = 1$ if and only if $x \in A$.] Then f is both one-to-one and onto. Hence $\mathscr{P}(X) \approx C(X)$.

6.8. Suppose A is an infinite set and F is a finite subset of A. Show that $A \backslash F \approx A$. In other words, removing a finite number of elements from an infinite set does not change its cardinality.

Suppose $F = \{a_1, a_2, \ldots, a_n\}$. Choose a denumerable subset $D = \{a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\}$ of A so that the first n elements of D are the elements of F. Let $g: A \to A \backslash F$ be defined by

$$g(a) = a \text{ if } a \notin D \qquad \text{and} \qquad g(a_k) = a_{k+n} \text{ if } a \in D$$

Then g is one-to-one correspondence between A and $A \backslash F$. Thus $A \approx A \backslash F$.

6.9. Prove Theorem 6.3: A subset of a denumerable set is either finite or denumerable.

Consider any denumerable set, say,

$$A = \{a_1, a_2, a_3, \ldots\} \tag{1}$$

Let B be a subset of A. If $B = \varnothing$, then B is finite. Suppose $B \neq 0$. Let b_1 be the first element in the sequence in (1) such that $b_1 \in B$; let b_2 be the first element which follows b_1 in the sequence in (1) such that $b_2 \in B$; and so on. Then $B = \{b_1, b_2, \ldots\}$. If the sequence $b_1, b_2, \ldots$ ends, then B is finite. Otherwise B is denumerable.

6.10. Prove: A countable union of finite sets is countable.

Let $\mathscr{C} = \{S_i : i \in \mathbf{P}\}$ be a countable collection of finite sets, and let $C = \cup_i S_i$. If C is empty, then C is countable. Suppose $C \neq \varnothing$. Define $A_1 = S_1$, $A_2 = S_2 \backslash S_1$, $A_3 = S_3 \backslash S_2$, and so on. Then the sets A_i are finite and pairwise disjoint. Say,

$$A_1 = \{a_{11}, a_{12}, \ldots, a_{1n_1}\}, \qquad A_2 = \{a_{21}, a_{22}, \ldots, a_{2n_2}\}, \ldots$$

Then the union $B = \cup_i A_i$ can be written as a sequence as follows:

$$B = \{a_{11}, a_{12}, \ldots, a_{1n_1}, a_{21}, a_{22}, \ldots, a_{2n_2}, \ldots\}$$

That is, first we write down the elements of A_1, then the elements of A_2, and so on. Formally, define $f: D \to \mathbf{P}$ as follows:

$$f(a_{ij}) = n_1 + n_2 + \cdots + n_{i-1+j}$$

Then f is bijective. Hence B is countable. However, B is also the union of the sets in $\mathscr{C}$; that is, $B = C$. Therefore, C is countable, as claimed.

6.11. Prove Theorem 6.5: Let $A_1, A_2, A_3, \ldots$ be a sequence of pairwise disjoint denumerable sets. Then the union $S = \cup_i A_i$ is denumerable.

Suppose

$$A_1 = \{a_{11}, a_{12}, a_{13}, \ldots\}, \qquad A_2 = \{a_{21}, a_{22}, a_{23}, \ldots\}, \quad \ldots$$

Define $D_n = \{a_{ij} : i + j = n, n > 1\}$. For example,

$$D_2 = \{a_{11}\}, \qquad D_3 = \{a_{12}, a_{21}\}, \qquad D_4 = \{a_{13}, a_{22}, a_{31}\}, \quad \ldots$$

Note that each D_n is finite. In fact, D_n has $n - 1$ elements. By Problem 6.10, $T = \bigcup(D_j : j > 1)$ is countable. On the other hand, the union of the finite D's is the same as the union of the A's, that is, $T = S$. Thus S is countable.

6.12. Show that $\mathbf{R} \approx \mathbf{R}^+$. (The sets of positive and negative real numbers are denoted, respectively, by $\mathbf{R}^+$ and $\mathbf{R}^-$.)

The function $f(x) = x/(1 + |x|)$ is a one-to-one correspondence between $\mathbf{R}^-$ and the open interval $(-1, 0)$. Hence the function h defined by

$$h(x) = \begin{cases} \dfrac{x}{1 + |x|} + 1 & \text{if } x < 0 \\ x + 1 & \text{if } x \geq 0 \end{cases}$$

is a one-to-one correspondence between $\mathbf{R}$ and $\mathbf{R}^+$. Hence $\mathbf{R} \approx \mathbf{R}^+$.

6.13. Suppose A is any uncountable set and B is a denumerable subset of A. Show that $A \backslash B \approx A$. In other words, removing a denumerable set from an uncountable set does not change its cardinality.

Suppose $B = \{b_1, b_2, b_3, \ldots\}$. The set $A \backslash B$ is infinite (indeed uncountable) and contains a denumerable subset, say, $D = \{d_1, d_2, d_3, \ldots\}$. Let $A^* = A \backslash (B \cup D)$. Then A and $A \backslash B$ are the following disjoint unions,

$$A = A^* \cup D \cup B = A^* \cup \{d_1, d_2, d_3, \ldots\} \cup \{b_1, b_2, b_3, \ldots\}$$
$$A \backslash B = A^* \cup D = A^* \cup \{d_1, d_2, d_3, \ldots\}$$

Define $f: A \to A \backslash B$ as in Fig. 6-6, that is,

$$\begin{aligned} f(a) &= a && \text{if } a \in A^* \\ f(d_n) &= d_{2n} - 1 && n \in \mathbf{P} \\ f(b_n) &= d_{2n} && n \in \mathbf{P} \end{aligned}$$

Then f is one-to-one and onto; hence $A \backslash B \approx A$.

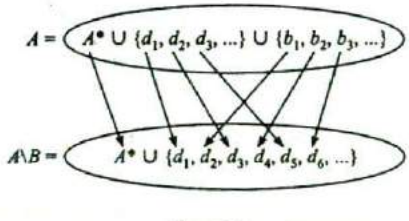


Fig. 6-6

6.14. Prove: The plane $\mathbf{R}^2$ is not the union of a countable number of lines.

Let $\mathscr{L}$ be any countable collection of lines. Since there are $\mathfrak{c}$ vertical lines and $\mathscr{L}$ is countable, there is a vertical line T such that $T \notin \mathscr{L}$. Now each line in $\mathscr{L}$ can intersect T in at most one point. Thus there are only a countable number of points in T which lie on lines in $\mathscr{L}$. Hence there is a point $p \in T \subseteq \mathbf{R}^2$ which does not line on any line in $\mathscr{L}$.

6.15. Prove Theorem 6.8: The unit interval $\mathbf{I} = [0, 1]$ is not denumerable.

Method 1: Assume $\mathbf{I}$ is denumerable. Then

$$\mathbf{I} = \{x_1, x_2, x_3, \ldots\}$$

that is, the elements of $\mathbf{I}$ can be written in a sequence.

Now each element in $\mathbf{I}$ can be written in the form of an infinite decimal as follows:

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots \\ x_2 &= 0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots \\ &\cdots\cdots\cdots\cdots \\ x_n &= 0.a_{n1}a_{n2}a_{n3}\cdots a_{nn}\cdots \\ &\cdots\cdots\cdots\cdots \end{aligned}$$

where $a_{ij} \in \{0, 1, \ldots, 9\}$ and where each decimal contains an infinite number of nonzero elements. Thus we write 1 as 0.999... and, for those numbers which can be written in the form of a decimal in two ways, for example,

$$1/2 = 0.5000\ldots = 0.4999\ldots$$

(in one of them there is an infinite number of nines and in the other all except a finite set of digits are zeros), we write the infinite decimal in which an infinite number of nines appear.

Now construct the real number

$$y = 0.b_1b_2b_3\cdots b_n\cdots$$

which will belong to $\mathbf{I}$, in the following way:

Choose b_1 so $b_1 \neq a_{11}$ and $b_1 \neq 0$. Choose b_2 so $b_2 \neq a_{22}$ and $b_2 \neq 0$. And so on.

Note $y \neq x_1$ since $b_1 \neq a_{11}$ (and $b_1 \neq 0$); $y \neq x_2$ since $b_2 \neq a_{22}$ (and $b_2 \neq 0$), and so on. That is, $y \neq x_n$ for all $n \in \mathbf{P}$. Thus $y \notin \mathbf{I}$, which contradicts the fact that $y \in \mathbf{I}$. Thus the assumption that $\mathbf{I}$ is denumerable has led to a contradiction. Consequently, $\mathbf{I}$ is nondenumerable.

Method 2: [This second proof of Theorem 6.8 uses Problem 6.17(*b*).]

Assume $\mathbf{I}$ is denumerable. Then, as above,

$$\mathbf{I} = \{x_1, x_2, x_3, \ldots\}$$

that is, the elements of $\mathbf{I}$ can be written in a sequence.

Now construct a sequence of closed intervals $I_1, I_2, \ldots$ as follows. Consider the following three closed subintervals of $[0, 1]$:

$$[0, 1/3], \qquad [1/3, 2/3], \qquad [2/3, 1] \tag{1}$$

where each has length $1/3$. Now x_1 cannot belong to all three intervals. (If x_1 is one of the endpoints, then it could belong to two of the intervals, but not all three.) Let $I_1 = [a_1, b_1]$, be one of the intervals in (*1*) such that $x_1 \notin I_1$. Now consider the following three closed subintervals of $I_1 = [a_1, b_1]$:

$$[a_1, a_1 + 1/9], \qquad [a_1 + 1/9,\ a_1 + 2/9], \qquad [a_1 + 2/9,\ b_1] \tag{2}$$

where each has length $1/9$. Similarly, let I_2 be one of the intervals in (*2*) with the property that x_2 does not belong to I_2. Continue in this manner. Thus we obtain a sequence of closed intervals,

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots \tag{3}$$

such that $x_n \notin I_n$ for all $n \in \mathbf{P}$.

By the above property of real numbers, there exists a real number $y \in \mathbf{I} = [0, 1]$ such that y belongs to every interval in (*3*). But since

$$y \in \mathbf{I} = \{x_1, x_2, x_3, \ldots\}$$

we must have $y = x_m$ for some $m \in \mathbf{P}$. By our construction $y = x_m \notin I_m$, which contradicts the fact that y belongs to every interval in (*3*). Thus our assumption that $\mathbf{I}$ is denumerable has led to a contradiction. Accordingly, $\mathbf{I}$ is nondenumerable.

6.16. Prove that $\mathbf{R}^2 \approx \mathbf{R}$ and, more generally, that $\mathbf{R}^n \approx \mathbf{R}$.

Since $\mathbf{R} \approx S = (0,1)$, it suffices to show that the open unit square

$$S^2 = \{(x,y) : 0 < x < 1,\ 0 < y < 1) = (0,1) \times (0,1)$$

has the same cardinality as $S = (0,1)$. Any point $(x,y) \in S$ can be written in the decimal form

$$(x,y) = (0.d_1d_2d_3\cdots, 0.e_1e_2e_3\cdots)$$

where each decimal expansion contains an infinite number of nonzero digits (e.g., for 1/2 write 0.4999... instead of 0.5000... 0. The function

$$f(x,y) = 0.d_1e_1d_2e_2d_3e_3\cdots$$

is one-to-one by the uniqueness of decimal expansions. Furthermore, the function $g: S \to S^2$ defined by $g(x) = (x, 1/2)$ is one-to-one. Accordingly, by the Schroeder–Bernstein Theorem 6.10, $S^2 \approx S$. Thus $\mathbf{R}^2 \approx \mathbf{R}$.

Therefore, $\mathbf{R}^3 \approx \mathbf{R}^2 \times \mathbf{R} \approx \mathbf{R} \times \mathbf{R} \approx \mathbf{R}$. Similarly, by induction, $\mathbf{R}^n \approx \mathbf{R}$.

6.17. A sequence $I_1, I_2, \ldots$ of intervals is said to be "nested" if $I_1 \supseteq I_2 \supseteq \ldots$.

(*a*) Give an example of a nested sequence of open intervals I_k whose intersection is empty.

(*b*) Prove the Nested Interval Property of the real numbers $\mathbf{R}$: A nested sequence $I_1 = [a_1, b_1]$, $I_2 = [a_2, b_2], \ldots$ of closed intervals is not empty.

(*a*) Let $I_k = (0, 1/k)$. Then $\bigcap(I_k : k \in P) = \varnothing$. [This follows from the fact that, for any $\varepsilon > 0$ there exists a k such that $1/k < \varepsilon$.]

(*b*) Let $A = \{a_1, a_2, \ldots\}$. Since the intervals are nested, A is bounded and every b_k is an upper bound of A. By the completion property of $\mathbf{R}$, $y = \sup(A)$ exists. Thus, for every k, $a_k \le y \le b_k$. Thus y belongs to every interval, and hence $\bigcap_k I_k \neq \varnothing$.

CARDINAL NUMBERS AND THE INEQUALITY OF CARDINAL NUMBERS

6.18. Prove Cantor's Theorem 6.9: For any set A, we have $|A| < |\mathscr{P}(A)|$.

The function $g: A \to \mathscr{P}(A)$ which sends each element $a \in A$ into the set consisting of a alone, i.e., which is defined by $g(a) = \{a\}$, is one-to-one. Thus $|A| \le |\mathscr{P}(A)|$.

If we now show that $|A| \neq |\mathscr{P}(A)|$, then the theorem will follow. Suppose the contrary, that is, suppose $|A| = |\mathscr{P}(A)|$ and that $f: A \to \mathscr{P}(A)$ is one-to-one and onto. Let $a \in A$ be called a "bad" element if a is member of the set which is its image, i.e., if $a \notin f(a)$. Now let B be the set of "bad" elements. That is,

$$B = \{x : x \in A, x \notin f(x)\}$$

Now B is a subset of A, that is, $B \in \mathscr{P}(A)$. Since $f: A \to \mathscr{P}(A)$ is onto, there exists an element $b \in A$ such that $f(b) = B$. Is b a "bad" element or a "good" element? If $b \in B$ then, by definition of B, $b \notin f(b) = B$, which is impossible. Likewise, if $b \notin B$, then $b \in f(b) = B$, which is also impossible. Thus the original assumption, that $|A| = |\mathscr{P}(A)|$, has led to a contradiction. Hence the assumption is false, and so the theorem is true.

6.19. Prove Theorem 6.11 (which is an equivalent formulation of the Schroeder–Bernstein theorem 6.10): Let X, Y, X_1 be sets such that $X \supseteq Y \supseteq X_1$ and $X \approx X_1$. Then $X \approx Y$.

Since $X \approx X_1$, there exists a one-to-one correspondence (bijection) $f: X \to X_1$. Since $X \supseteq Y$, the restriction of f to Y, which we also denote by f, is also one-to-one. Let $f(Y) = Y_1$. Then Y and Y_1 are equipotent,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1$$

and $f: Y \to Y_1$ is bijective. But now $Y \supseteq X_1 \supseteq Y_1$ and $Y \approx Y_1$. For similar reasons, X_1 and $f(X_1) = X_2$ are equipotent,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2$$

and $f: X_1 \to X_2$ is bijective. Accordingly, there exist equipotent sets $X, X_1, X_2, \ldots$ and equipotent sets $Y, Y_1, Y_2, \ldots$ such that

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2 \supseteq Y_2 \supseteq X_3 \supseteq Y_3 \supseteq \cdots$$

and $f: X_k \to X_{k+1}$ and $f: Y_k \to Y_{k+1}$ are bijective.

Let

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \cdots$$

Then

$$X = (X \setminus Y) \cup (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup \cdots \cup B$$
$$Y = (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup (Y_1 \setminus X_2) \cup \cdots \cup B$$

Furthermore, $X \setminus Y, X_1 \setminus Y_1, X_2 \setminus Y_2, \ldots$ are equipotent. In fact, the function

$$f: (X_k \setminus Y_k) \to (X_{k+1} \setminus Y_{k+1})$$

is one-to-one and onto.

Consider the function $g: X \to Y$ defined by the diagram in Fig. 6-7. That is,

$$g(x) = \begin{cases} f(x) & \text{if } x \in X_k \setminus Y_k \text{ or } x \in X \setminus Y \\ x & \text{if } x \in Y_k \setminus X_k \text{ or } x \in B \end{cases}$$

Then g is one-to-one and onto. Therefore $X \approx Y$.

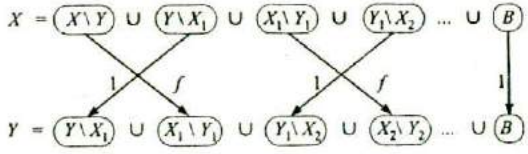


Fig. 6-7

6.20. Prove Theorem 6.13: $\mathfrak{c} = 2^{\aleph_0}$.

Let $\mathbf{R}$ be the set of real numbers and let $\mathscr{P}(\mathbf{Q})$ be the power set of the set $\mathbf{Q}$ of rational numbers, i.e., the family of subsets of $\mathbf{Q}$. Furthermore, let the function $f: \mathbf{R} \to \mathscr{P}(\mathbf{Q})$ be defined by

$$f(a) = \{x : x \in \mathbf{Q}, x < a\}$$

That is, f maps each real number a into the set of rational numbers less than a. We shall show that f is one-to-one. Let $a, b \in \mathbf{R}$, $a \neq b$ and, say, $a < b$. By a property of the real numbers, there exists a rational number r such that

$$a < r < b$$

Then $r \in f(b)$ and $r \notin f(a)$; hence $f(b) \neq f(a)$. Therefore, f is one-to-one. Thus $|\mathbf{R}| \leq |\mathscr{P}(\mathbf{Q})|$. Since $|\mathbf{R}| = \mathfrak{c}$ and $|\mathbf{Q}| = \aleph_0$, we have

$$\mathfrak{c} \leq 2^{\aleph_0}$$

Now let $C(\mathbf{P})$ be the family of characteristic functions $f: \mathbf{P} \to \{0, 1\}$ which, as proven in Problem 6.8, is

equivalent to $\mathscr{P}(\mathbf{P})$. Here $\mathbf{P} = \{1, 2, \ldots\}$. Let $\mathbf{I} = [0, 1]$, the closed unit interval, and let the function $F : C(\mathbf{P}) \to \mathbf{I}$ be defined by

$$F(f) = 0.f(1)f(2)f(3)\cdots$$

an infinite decimal consisting of zeros or ones. Suppose $f, g \in C(\mathbf{P})$ and $f \neq g$. Then the decimals would be different, and so $F(f) \neq F(g)$. Accordingly, F is one-to-one. Therefore,

$$|\mathscr{P}(\mathbf{Q})| = |C(\mathbf{P})| \leq |\mathbf{I}|$$

Since $|\mathbf{Q}| = \aleph_0$ and $|\mathbf{I}| = \mathfrak{c}$, we have

$$2^{\aleph_0} \leq \mathfrak{c}$$

Both inequalities give us

$$\mathfrak{c} = 2^{\aleph_0}$$

6.21. Let $S = (0, 1)$, the open unit interval, and let T be the set of real numbers in S which have an infinite number of threes in their decimal expansion. Show that $|T| = |S|$.

Let $x \in S$ and suppose $x = 0.d_1d_2d_3\cdots d_n\cdots$. Let the function $f: S \to T$ be defined by

$$f(x) = 0.d_1 3 d_2 3 d_3 3 \cdots 3 d_n 3 \cdots$$

Then f is one-to-one and hence $|S| \leq |T|$. Since T is a subset of S, we have $|T| \leq |S|$. By the Schroeder–Bernstein theorem, $|T| = |S|$.

6.22. Let S denote the open unit interval $(0, 1)$, and let S^ω denote the set of all denumerable sequences $(x_1, x_2, x_3, \ldots)$ where $x_i \in S$. (*a*) Prove $|S^\omega| \approx |S|$. (*b*) Prove the set $\mathbf{R}^\omega$ of all denumerable sequences of real numbers has cardinality $\mathfrak{c}$.

(*a*) Let $(x_1, x_2, x_3, \ldots) \in S^\omega$. Consider the decimal expansions:

$$x_1 = 0.d_{11}d_{12}d_{13}d_{14}\cdots$$
$$x_2 = 0.d_{21}d_{22}d_{23}d_{24}\cdots$$
$$x_3 = 0.d_{31}d_{32}d_{33}d_{34}\cdots$$
And so on

Associate the sequence $(x_1, x_2, x_3, \ldots)$ with the decimal number

$$0.d_{11} : d_{21}d_{12} : d_{13}d_{22}d_{31} : \cdots$$

where the subscripts in the successive blocks of digits $d_{11}, d_{22}d_{12}, d_{13}d_{22}d_{31}, \ldots$ are obtained by "following the arrows" in Fig. 6-1. (This procedure was used to show that $\mathbf{P} \times \mathbf{P}$ is countable.) This association defines a one-to-one function from S^ω into S. The function $g : S \to S^\omega$ defined by $f(x) = (x, x, x, \ldots)$ is also one-to-one. By the Schroeder–Bernstein theorem $|S^\omega| \approx |S|$.

(*b*) Since $\mathbf{R} \approx S$, it follows that $|\mathbf{R}^\omega| = |S^\omega| = |S| = \mathfrak{c}$.

CARDINAL ARITHMETIC

6.23. Let A_1, A_2, A_3, A_4 be any sets. Define sets B_1, B_2, B_3, B_4 such that

$$|A_1| + |A_2| + |A_3| + |A_4| = |B_1 \cup B_2 \cup B_3 \cup B_4|$$

Let $B_1 = A_1 \times \{1\}$, $B_2 = A_2 \times \{2\}$, $B_3 = A_3 \times \{3\}$, $B_4 = A_4 \times \{4\}$. Then $B_k \approx A_k$ for $k = 1, 2, 3, 4$. Also, the B_k are disjoint, that is, $B_i \cap B_j = \varnothing$ if $i \neq j$. Consequently, the above will be true.

6.24. Let $\{A_i : i \in I\}$ be any family of sets. Define a family of sets $\{B_i : i \in I\}$ such that $B_i \approx A_i$, for $i \in I$, and $B_i \cap B_j = \varnothing$ for $i \neq j$.

Let $B_i = A_i \times \{i\}$. Then the family $\{B_i : i \in I\}$ has the required properties.

6.25. Prove Theorem 6.14: The addition and multiplication of cardinal numbers satisfy the properties in Table 6-1. That is, for cardinal numbers α, β, γ:

(1) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
(2) $\alpha + \beta = \beta + \alpha$
(3) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$
(4) $\alpha\beta = \beta\alpha$
(5) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$
(6) If $\alpha \leq \beta$, then $\alpha + \gamma \leq \beta + \gamma$
(7) If $\alpha \leq \beta$, then $\alpha\gamma \leq \beta\gamma$

Let A, B, C be pairwise disjoint sets such that $\alpha = |A|$, $\beta = |B|$, $\gamma = |C|$.

(1) We have:

$$(\alpha + \beta) + \gamma = |A \cup B| + |C| = |(A \cup B) \cup C|$$
$$\alpha + (\beta + \gamma) = |A| + |B \cup C| = |A \cup (B \cup C)|$$

However, the union of sets is associative, i.e., $(A \cup B) \cup C = A \cup (B \cup C)$. Hence

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

(2) Since $A \cup B = B \cup A$, we have

$$\alpha + \beta = |A \cup B| = |B \cup A| = \beta + \alpha$$

(3) We have:

$$(\alpha\beta)\gamma = |A \times B||C| = |(A \times B) \times C|$$
$$\alpha(\beta\gamma) = |A||B \times C| = |A \times (B \times C)|$$

However, by Problem 6.6(b), $(A \times B) \times C \approx A \times (B \times C)$. Hence

$$(\alpha\beta)\gamma = \alpha(\beta\gamma)$$

(4) By Problem 6.6(a), $A \times B \approx B \times A$; hence

$$\alpha\beta = |A \times B| = |B \times A| = \beta\alpha$$

(5) Note first that $B \cap C = \varnothing$ implies $(A \times B) \cap (A \times C) = \varnothing$. Then:

$$\alpha(\beta + \gamma) = |A||B \cup C| = |A \times (B \cup C)|$$
$$\alpha\beta + \alpha\gamma = |A \times B| + |A \times C| = |(A \times B) \cup (A \times C)|$$

However, $A \times (B \cup C) = (A \times B) \cup (A \times C)$. Therefore,

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$$

(6) Suppose $\alpha \leq \beta$. Then there exists a one-to-one mapping $f: A \to B$. Let $g : A \cup C \to B \cup C$ be defined by

$$g(x) = \begin{cases} f(x) & \text{if } x \in A \\ x & \text{if } x \in C \end{cases}$$

Then g is one-to-one. Accordingly, $|A \cup C| \leq |B \cup C|$ and so

$$\alpha + \gamma \leq \beta + \gamma$$

(7) Suppose $\alpha \leq \beta$. Then there exists a one-to-one mapping $f: A \to B$. Let $g : A \times C \to B \times C$ be defined by

$$g(a, c) = (f(a), c)$$

Then g is one-to-one. Accordingly, $|A \times C| \leq |B \times C|$ and so

$$\alpha\gamma \leq \beta\gamma$$

6.26. Prove: $\aleph_0 \mathbf{c} = \mathbf{c}$.

Consider the integers $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and the half-open interval $A = [0, 1)$. Furthermore, let $f: \mathbf{Z} \times A \to \mathbf{R}$ be defined by

$$f(n, a) = n + a$$

In other words, $f(\{n\} \times [0, 1))$ is mapped onto $[n, n + 1)$. Then f is a one-to-one correspondence between $\mathbf{Z} \times A$ and $\mathbf{R}$. Since $|\mathbf{Z}| = \aleph_0$ and $|A| = |\mathbf{R}| = \mathbf{c}$, we have

$$\aleph_0 \mathbf{c} = |\mathbf{Z} \times A| = |\mathbf{R}| = \mathbf{c}$$

6.27. Prove: Let α be any infinite cardinal number. Then $\aleph_0 + \alpha = \alpha$.

We have shown that $\aleph_0 + \aleph_0 = \aleph_0$. Suppose α is uncountable, and $\alpha = |A|$. By Problem 6.13, $A \backslash B \approx A$ where B is a denumerable subset of A. Recall $A = (A \backslash B) \cup B$ and the union is disjoint. Hence

$$\alpha = |A| = |(A \backslash B) \cup B| = |A \backslash B| + |B| = \alpha + \aleph_0 = \aleph_0 + \alpha$$

MISCELLANEOUS PROBLEMS

6.28. Prove: The set $\mathscr{P}$ of all polynomials

$$p(x) = a_0 + a_1 x + a_2 x^2 + a_m x^m \tag{1}$$

with integral coefficients, that is, where $a_0, a_1, \ldots, a_m$ are integers, is denumerable.

For each pair of nonnegative integers (n, m), let $P(n, m)$ be the set of polynomials in (1) of degree m in which

$$|a_0| + |a_1| + \cdots + |a_m| = n$$

Note that $P(n, m)$ is finite. Therefore

$$\mathscr{P} = \bigcup (P(n, m) : (n, m) \in \mathbf{N} \times \mathbf{N})$$

is countable since it is a countable family of countable sets. But $\mathscr{P}$ is not finite; hence $\mathscr{P}$ is denumerable.

6.29. A real number r is called an *algebraic* number if r is a solution to a polynomial equation

$$p(x) = a_0 + a_1 x + a_2 x^2 + a_m x^m = 0$$

with integral coefficients. Prove the set A of algebraic numbers is denumerable.

By the preceding Problem 6.28, that the set E of polynomial equations is denumerable:

$$E = \{p_1(x) = 0,\ p_2(x) = 0,\ p_3(x) = 0, \ldots\}$$

Define

$$A_k = \{x : x \text{ is a solution of } p_k(x) = 0\}$$

Since a polynomial of degree n can have at most n roots, each A_k is finite. Therefore

$$A = \bigcup \{A_k : k \in \mathbf{P}\}$$

is a countable family of countable sets. Accordingly, A is countable and, since A is not finite, A is denumerable.

6.30. Explicitly exhibit $\aleph_0$ pairwise-disjoint denumerable subsets of $\mathbf{P} = \{1, 2, 3, \ldots\}$.

Let p and q be distinct prime numbers. The sets

$$S_p = \{p, p^2, p^3, \ldots\} \qquad \text{and} \qquad S_q = \{q, q^2, q^3, \ldots\}$$

are pairwise disjoint. One can show that the set $\{p_1, p_2, p_3, \ldots\}$ of prime numbers is an infinite subset of $\mathbf{P}$ and hence has cardinality $\aleph_0$. Thus the family $\{S_{p_1}, S_{p_2}, S_{p_3}, \ldots\}$ has the desired properties.

Supplementary Problems

EQUIPOTENT SETS, COUNTABLE SETS, CONTINUUM

6.31. The set **Z** of integers can be put into a one-to-one correspondence with $\mathbf{P} = \{1, 2, 3, \ldots\}$ as follows:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \ldots \end{array}$$

Find a formula for the function $f: \mathbf{P} \to \mathbf{Z}$ which gives the above correspondence between **P** and **Z**.

6.32. $\mathbf{P} \times \mathbf{P}$ was written as a sequence by considering the diagram in Fig. 6-1. This is not the only way to write $\mathbf{P} \times \mathbf{P}$ as a sequence. Write $\mathbf{P} \times \mathbf{P}$ as a sequence in two other ways by drawing appropriate diagrams.

6.33. Prove that the set S of rational points in the plane $\mathbf{R}^2$ is denumerable. [A point $p = (x, y)$ in $\mathbf{R}^2$ is rational if x and y are rational.]

6.34. Let S be the set of rational points in the plane $\mathbf{R}^2$. Show that S can be partitioned into two sets V and H such that the intersection of V with any vertical line is finite and the intersection of H with any horizontal line is finite.

6.35. Let $\mathscr{A} = \{A_i : i \in I\}$ be a set of pairwise disjoint intervals in the line **R**. Show that $\mathscr{A}$ is countable.

6.36. Let $\mathscr{B} = \{B_i : i \in I\}$ be a set of pairwise disjoint circles in the plane $\mathbf{R}^2$. Show that $\mathscr{B}$ is countable.

6.37. A function $f: \mathbf{P} \to \mathbf{P}$ is said to have finite support if $f(n) = 0$ for all but a finite number of n. Show that the set of all such functions is denumerable.

6.38. A real number x is called *transcendental* if x is not algebraic, i.e., if x is not a solution to a polynomial equation

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

with integral coefficients. (See Problem 6.29.) For example, π and e are transcendental numbers. Prove that the set T of transcendental numbers has the power of the continuum.

6.39. Recall that a *permutation* of $\mathbf{P} = \{1, 2, 3, \ldots\}$ is a bijective function $\sigma : \mathbf{P} \to \mathbf{P}$. Show that the set PERM(**P**) of all permutations of **P** has the power of the continuum.

CARDINAL NUMBERS, CARDINAL ARITHMETIC

6.40. Suppose α and β are cardinal numbers such that $\alpha \leq \beta$. Show that there exists a set S with a subset A such that $\alpha = |A|$ and $\beta = |S|$.

6.41. Show that Theorems 6.10 and 6.11 are equivalent. (Hence each proves the Schroeder–Bernstein theorem.)

6.42. Prove $\mathbf{c}^{\aleph_0} = \mathbf{c}$.

6.43. Show that there are only $\mathbf{c}$ continuous functions from **R** into **R**. (Assume that if f and g are such continuous functions and $f(q) = g(q)$ for all rational numbers q in **R**, then $f = g$, that is, $f(x) = g(x)$ for all x in **R**.)

6.44. Prove Theorem 6.16(2): Let α, β, γ be cardinal numbers. Then $\alpha^\beta \alpha^\gamma = \alpha^{\beta+\gamma}$.

6.45. Let α, β, γ be cardinal numbers such that $\alpha \leq \beta$. Prove: (*a*) $\alpha^\gamma \leq \beta^\gamma$, (*b*) $\gamma^\alpha \leq \gamma^\beta$.

6.46. Show that the cardinal inequality relations are well defined; that is, if $A \approx A'$ and $B \approx B'$, show that:

(*a*) $|A| \leq |B|$ if and only if $|A'| \leq |B'|$. (*b*) $|A| < |B|$ if and only if $|A'| < |B'|$.

6.47. Show that cardinal addition and multiplication are well defined, that is:

(*a*) *Cardinal Addition*: If $A \approx A'$ and $B \approx B'$, where A and B are disjoint and A' and B' are disjoint, show that $|A \cup B| = |A' \cup B'|$.

(*b*) *Cardinal Multiplication*: If $A \approx A'$ and $B \approx B'$, show that $|A \times B| = |A' \times B'|$.

6.48. Let $\mathscr{C}$ be the collection of all circles in the plane $\mathbf{R}^2$. Show that $\mathscr{C}$ has cardinality $\mathfrak{c}$.

MISCELLANEOUS PROBLEMS

6.49. (Heine–Borel Property of the real numbers $\mathbf{R}$.) Let $\mathscr{C} = \{I_k : k \in K\}$ be a collection of open intervals which covers a closed interval $A = [a, b]$. Show that $\mathscr{C}$ contains a finite subcover of A, that is, a finite subcollection of $\mathscr{C}$ is a cover of A. [A collection $\{I_k : k \in K\}$ of intervals is called a "cover" of a set A if $A \subseteq \bigcup_k I_k$.]

Answers to Supplementary Problems

6.31. The following function $f: \mathbf{P} \to \mathbf{P}$ has the required property:

$$f(n) = \begin{cases} -n/2 + 1/2 & \text{if } n \text{ is odd} \\ n/2 & \text{if } n \text{ is even} \end{cases}$$

6.32. Each diagram in Fig. 6-8 shows that $\mathbf{P} \times \mathbf{P}$ can be written as an infinite sequence of distinct elements as follows:

(*a*) $\mathbf{P} \times \mathbf{P} = \{(1,1), (2,1), (2,2), (1,2), (1,3), (2,3), \ldots\}$

(*b*) $\mathbf{P} \times \mathbf{P} = \{(1,1), (1,2), (2,1), (1,3), (2,2), (3,1), (1,4), \ldots\}$

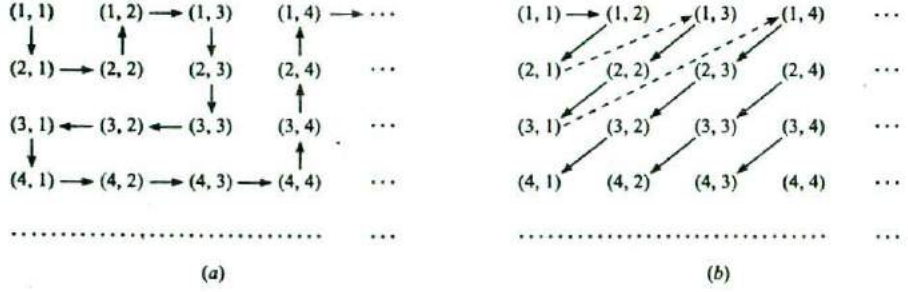


Fig. 6-8

6.33. $|\mathbf{Q} \times \mathbf{Q}| = |\mathbf{P} \times \mathbf{P}| = |\mathbf{P}| = \aleph_0$

6.35. *Hint*: Each interval contains a distinct rational number.

6.36. *Hint*: Each circle contains a distinct rational point in $\mathbf{R}^2$.

6.38. *Hint*: $\mathbf{R}$ is the union of the algebraic and transcendental numbers.

6.42. *Hint*: Use Problem 6.22

6.43. *Hint*: Use Problem 6.22 or 6.42.

6.44. *Hint*: Let $\alpha = |A|, \beta = |B|, \gamma = |C|$ where B and C are disjoint. Let $D = B \cup C$. Then $\beta + \gamma = |B \cup C| = |D|$. Associate with each function $f: D \to A$ the pair $f_1: B \to A$ and $f_2: C \to A$ where $f_1 = f|_B$ and $f_2 = f|_C$. Show that the map $F(f) = (f_1, f_2)$ is bijective.

6.45. *Hint*: Let $\alpha = |A|, \beta = |B|, \gamma = |C|$ where we can assume $A \subseteq B$ since $\alpha \leq \beta$.

(*a*) For each function $f: C \to A$ associate the function $f': C \to B$ defined by $f'(x) = f(x)$. Show that the map $F(f) = g$ is one-to-one.

(*b*) For each function $f: A \to C$ associate a function $f': B \to C$ which extends f, i.e., for each $a \in A$, $f'(a) = f(a)$. Show that the map $F(f) = f'$ is one-to-one.

6.48. Since each circle in $\mathscr{C}$ is determined by its center (x, y) and radius r, $\mathscr{C} \approx \mathbf{R} \times \mathbf{R} \times \mathbf{R}^+ \approx \mathbf{R}$.

6.49. Suppose no finite subcollection of $\mathscr{C}$ is a cover of A. Let p_1 be the midpoint of the interval $A = A_1 = [a_1, b_1]$. At least one of $[a_1, p_1]$ and $[p_1, b_1]$ cannot be covered by a finite subcollection of $\mathscr{C}$ or else the whole interval A_1 will be, and let $A_2 = [a_2, b_2]$ be that subinterval. Similarly, let p_2 be the midpoint of the interval $A_2 = [a_2, b_2]$, and let $A_3 = [a_3, b_3]$ be one of the two intervals $[a_2, p_2]$ and $[p_2, b_2]$ which cannot be covered by a finite subcollection of $\mathscr{C}$, and so on. Thus we have a sequence $A_1, A_2, \ldots$ of nested closed intervals, and each cannot be covered by a finite subcollection of $\mathscr{C}$. Furthermore, $\lim_{n \to \infty} d_n = 0$ where $d_n = b_n - a_n$ is the length of A_n. By Problem 6.17(*b*), there exists a real number y in every A_k. Since $\mathscr{C}$ is a cover of A, y belongs to some element of $\mathscr{C}$, say $y \in I_j$ where $I_j = (c, d)$. Let e be the distance from y to the closest endpoint of I_j. Then there exists d_j such that $d_j < e$. This means $A_j \subseteq I_j$. This contradicts the fact that A_j cannot be covered by a finite subcollection of $\mathscr{C}$. Thus the original assumption that no finite subcollection of $\mathscr{C}$ covers A leads to a contradiction, and so a finite subcollection of $\mathscr{C}$ covers A.

Chapter 7

Ordered Sets and Lattices

7.1 INTRODUCTION

Order and precedence relationships appear in many different places in mathematics and computer science. This chapter makes these notions precise. We also define a lattice, which is a special kind of an ordered set.

7.2 ORDERED SETS

Suppose R is a relation on a set S satisfying the following three properties:

$[O_1]$ (***Reflexive***): For any $a \in S$, we have $a R a$.

$[O_2]$ (***Antisymmetric***): If $a R b$ and $b R a$, then $a = b$.

$[O_3]$ (***Transitive***): If $a R b$ and $b R c$, then $a R c$.

Then R is called a *partial order* or, simply an *order* relation, and R is said to define a *partial ordering* of S. The set S with the partial ordering R is called a *partially ordered set* or, simply, an *ordered set*. (Sometimes the term *poset* is used for partially ordered set.)

The most familiar order relation, called the *usual order*, is the relation $\leq$ (read "less than or equal") on the positive integers $\mathbf{P}$ or, more generally, on any subset of the real numbers $\mathbf{R}$. For this reason, a partial ordering relation is frequently denoted by

$$\preceq$$

With this notation, the above three properties of a partial order appear in the following usual form:

$[O_1]$ (***Reflexive***): For any $a \in S$, we have $a \preceq a$.

$[O_2]$ (***Antisymmetric***): If $a \preceq b$ and $b \preceq a$, then $a = b$.

$[O_3]$ (***Transitive***): If $a \preceq b$ and $b \preceq c$, then $a \preceq c$.

Although an ordered set consists of two things, a set S and the partial ordering $\preceq$, one usually simply writes S to denote the ordered sets as long as the partial ordering is fixed in the context of the discussion; otherwise the ordered set is denoted by the pair $(S, \preceq)$.

Suppose S is an ordered set. Then the statement

$$a \preceq b \qquad \text{is read "}a \textit{ precedes } b\text{"}$$

In this context we also write:

$a \prec b$ means $a \preceq b$ and $a \neq b$; read "a strictly precedes b".

$b \succeq a$ means $a \preceq b$; read "b succeeds a".

$b \succ a$ means $a \prec b$; read "b strictly succeeds a".

$\npreceq$, $\nprec$, $\nsucceq$ and $\nsucc$ are self-explanatory.

When there is no ambiguity, the symbols $\leq$, $<$, $>$, $\geq$ are frequently used instead of $\preceq$, $\prec$, $\succ$, and $\succeq$, respectively.

EXAMPLE 7.1

(*a*) Let $\mathscr{S}$ be any collection of sets. The relation $\subseteq$ of set inclusion is a partial ordering of $\mathscr{S}$. Specifically, $A \subseteq A$ for any set A; if $A \subseteq B$ and $B \subseteq A$ then $A = B$; and if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

(*b*) Consider the set **P** of positive integers. We say "a divides b", written $a|b$, if there exists an integer c such that $ac = b$. For example, $2|4$, $3|12$, $7|21$, and so on. This relation of divisibility is a partial ordering of **P**.

(*c*) The relation "|" of divisibility is not an ordering of the set **Z** of integers. Specifically, the relation is not antisymmetric. For instance, $2|-2$ and $-2|2$, but $2 \neq -2$.

(*d*) Consider the set **Z** of integers. Define $a \, R \, b$ if there is a positive integer r such that $b = a^r$. For instance, $2 \, R \, 8$ since $8 = 2^3$. One can show (Problem 7.8) that R is a partial ordering of **Z**.

Dual Order

Let $\precsim$ be any partial ordering of a set S. The relation $\succsim$, that is, a succeeds b, is also a partial ordering of S; it is called the *dual order*. Observe that $a \precsim b$ if and only if $b \succsim a$; hence the dual order $\succsim$ is the inverse of the relation $\precsim$, that is $\succsim \, = \, \precsim^{-1}$.

Ordered Subsets

Let A be a subset of an ordered set S, and suppose $a, b \in A$. Then the order in S induces an order in A in the following natural way:

$$a \precsim b \text{ as elements of } A \text{ whenever } a \precsim b \text{ as elements of } S$$

More precisely, if R is a partial ordering of S, then the relation

$$R_A = R \cap (A \times A)$$

is a partial ordering of A called the *induced order* on A or the *restriction* of R to A. The subset A with the induced order is called an *ordered subset* of S. Unless otherwise stated or implied, any subset of an ordered set S will be treated as an ordered subset of S.

Quasi-order

Suppose $\prec$ is a relation on a set S satisfying the following two properties:

$[Q_1]$ (***Irreflexive***): For any $a \in A$, we have $a \not\prec a$.
$[Q_2]$ (***Transitive***): If $a \prec b$, and $b \prec c$, then $a \prec c$.

Then $\prec$ is called a *quasi-order* on S.

There is a close relationship between partial orders and quasi-orders. Specifically, if $\precsim$ is a partial order on a set S and we define $a \prec b$ to mean $a \precsim b$ but $a \neq b$, then $\prec$ is a quasi-order on S. Conversely, if $\prec$ is a quasi-order on a set S and we define $a \precsim b$ to mean $a \prec b$ or $a = b$, then $\precsim$ is a partial order on S. This allows us to switch back and forth between a partial order and its corresponding quasi-order using whichever is more convenient.

Comparability

Suppose a and b are distinct elements in a partially ordered set S. We say a and b are *comparable* if

$$a \prec b \quad \text{or} \quad b \prec a$$

that is, if one of them precedes the other. Thus a and b are *noncomparable*, written

$$a \| b$$

if $a \not\prec b$ and $b \not\prec a$.

Linearly Ordered Sets

The word "partial" is used in defining a partially ordered set S since some of the elements of S need not be comparable. Suppose, on the other hand, every pair of elements of S are comparable. Then S is said to be *linearly* or *totally ordered*. Although an ordered set S may not be linearly ordered, it is still possible for a subset A of S to be linearly ordered. Such a linearly ordered subset A of an ordered set S is called a *chain* in S. Clearly, every subset of a linearly ordered set S must also be linearly ordered.

EXAMPLE 7.2

(*a*) Consider the set **P** of positive integers ordered by divisibility. Then 21 and 7 are comparable since 7|21. On the other hand, 3 and 5 are noncomparable since neither 3|5 nor 5|3. Thus **P** is not linearly ordered by divisibility. Observe that $A = \{2, 6, 12, 36\}$ is a chain (linearly ordered subset) in **P** since 2|6, 6|12, and 12|36.

(*b*) The set **P** of positive integers with the usual order $\leq$ (less than or equal) is linearly ordered and hence every ordered subset of **P** is also linearly ordered.

(*c*) The power set $\mathscr{P}(A)$ of a set A with 2 or more elements is not linearly ordered by set inclusion. For instance, suppose a and b belong to A. Then $\{a\}$ and $\{b\}$ are noncomparable. Observe that the empty set $\varnothing$, $\{a\}$, and A do form a chain in $\mathscr{P}(A)$ since $\varnothing \subseteq \{a\} \subseteq A$. Similarly, $\varnothing$, $\{b\}$, and A form a chain in $\mathscr{P}(A)$.

7.3 SET CONSTRUCTIONS AND ORDER

This section discusses different ways of defining an order on a set which is constructed from ordered sets.

Product Sets and Order

There are a number of ways to define an order relation on the cartesian product of given ordered sets. Two of these ways follow:

(*a*) ***Product Order***: Suppose S and T are ordered sets. Then the following, is an order relation on the product set $S \times T$, called the *product order*:

$$(a, b) \precsim (a', b') \qquad \text{if } a \leq a' \text{ and } b \leq b'$$

Problem 7.15 shows that this relationship does satisfy the necessary axioms of an order.

(*b*) ***Lexicographical Order***: Suppose S and T are linearly ordered sets. Then the following is an order relation on the product set $S \times T$, called the *lexicographical* or *dictionary order*:

$$(a, b) \prec (a', b') \begin{cases} \text{if } a < a', \\ \text{or if } a = a' \text{ and } b < b' \end{cases}$$

This order can be extended to $S_1 \times S_2 \times \cdots \times S_n$ as follows:

$$(a_1, a_2, \ldots, a_n) \prec (a_1', a_2', \ldots, a_n')$$
$$\text{if } a_1 = a_1', a_2 = a_2', \ldots, a_{k-1} = a_{k-1}', \text{ but } a_k < a_k'$$

Note that the lexicographical order is also linear.

Concatenation or Sum Order

Suppose $\{A_i : i \in I\}$ is a linearly ordered collection of disjoint linearly ordered sets; that is, the index set I is linearly ordered, each set A_i is linearly ordered, and $A_i \cap A_j = \varnothing$ when $i \neq j$. Then we assume, unless otherwise specified, the following linear order on the union $S = \bigcup_i A_i$, which we call the *concatenation order* or *usual order* or *sum order*:

$$x \prec y \begin{cases} \text{if } x \in A_i,\ y \in A_j, \text{ and } i < j \\ \text{or if } x, y \in A_i \text{ and } x < y \text{ as elements of } A_i \end{cases}$$

This order can sometimes be pictured by listing the elements of A_i before the elements A_j when $i < j$ and separating the sets by semicolons. For example, consider the sets

$$A = \{1, 3, 5, 7, \ldots\}, \qquad B = \{a, b, c\}, \qquad C = \{2, 4, 6, \ldots\}$$

where position in each set determines the linear order. Then the concatenation order on $S = A \cup B \cup C$ (where we assume the sets are ordered by the position in the union, i.e., $A < B < C$) may be pictured by writing

$$S = \{1, 3, 5, \ldots; a, b, c; 2, 4, 6, \ldots\}$$

Note that the order on $S' = B \cup A \cup C$ may be pictured by

$$S' = \{a, b, c; 1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

and this is not the same as the order on S.

Kleene Closure and Order

Let A be a nonempty linearly ordered set (sometimes called an *alphabet*). A *word* w over A is a finite sequence

$$w = a_1 a_2, \ldots, a_n$$

of elements of A. We will let $|w|$ denote the *length* n of w. (The empty sequence, denoted by λ, is also a word and $|\lambda| = 0$.) The Kleene closure of A, denoted by A^*, is defined to be the collection of all such words over A^*. The following are two order relations on A^*.

(*a*) ***Alphabetical (Lexicographical) Order***: The reader is no doubt familiar with the usual alphabetical ordering of A^*. That is:

(i) $\lambda < w$, where λ is the empty word and w is any nonempty word.

(ii) Suppose $u = au'$ and $v = bv'$ are distinct nonempty words where $a, b \in A$ and $u', v' \in A^*$. Then:

$$u \prec v \begin{cases} \text{if } a < b \\ \text{or if } a = b \text{ but } u' \prec v' \end{cases}$$

(*b*) ***Short-lex Order***: Here A^* is ordered first by length, and then alphabetically. That is, for any distinct words $u, v \in A^*$:

$$u \prec v \begin{cases} \text{if } |u| < |v| \\ \text{or if } |u| = |v| \text{ but } u \text{ precedes } v \text{ alphabetically} \end{cases}$$

For example, "to" precedes "and" since |"to"| = 2 but |"and"| = 3. However, "an" precedes "to" since they have the same length, but "an" precedes "to" alphabetically. This order is also called the *free semigroup order*.

7.4 PARTIALLY ORDERED SETS AND HASSE DIAGRAMS

Let S be a partially ordered set, and suppose $a, b \in S$. We say that a is an *immediate predecessor* of b, or that b is an *immediate successor* of a, or that b is a *cover* of a, written

$$a << b$$

if $a < b$ but no element in S lies between a and b, that is, there exists no element c in S such that $a < c < b$.

Suppose S is a finite partially ordered set. Then the order on S is completely known once we know all pairs a, b in S such that $a << b$, that is, once we know the relation $<<$ on S. This follows from the fact that $x < y$ if and only if $x << y$ or there exist elements $a_1, a_2, \ldots, a_m$ in S such that

$$x << a_1 << a_2 << \cdots << a_m << y$$

Hasse Diagrams

The *Hasse diagram* of a finite partially ordered set S is a graphical representation of S as follows. The elements of S are represented by points in the plane (called *vertices*), and there is a directed line segment (*arrow*) drawn from a to b (called an *edge*) whenever $a << b$ in S. Instead of drawing an arrow from a to b, we sometimes place b higher than a and draw a line between them. It is then understood that movement upwards indicates succession. In the diagram thus created, $x < y$ if and only if there is a directed path (sequence of edges) from vertex x to vertex y. Also, there can be no (directed) cycles in the diagram of S since the order relation is antisymmetric.

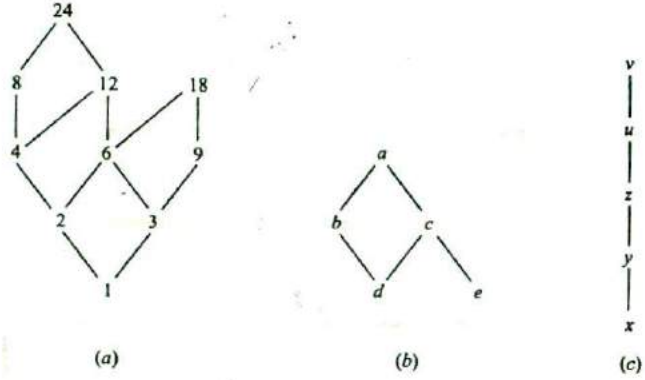
The Hasse diagram of an ordered set S is a picture of S; hence it is very useful in describing types of elements in S. Sometimes we define a partially ordered set by simply presenting its Hasse diagram.

EXAMPLE 7.3

(*a*) Let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ be ordered by the relation "x divides y". The Hasse diagram of A appears in Fig. 7-1(*a*).

(*b*) Let $B = \{a, b, c, d, e\}$. The diagram in Fig. 7-1(*b*) defines a partial ordering on B in a natural way. That is, $d \le b$, $d \le a$, $e \le c$, and so on. Note that b and c are noncomparable.

(*c*) The diagram of a finite linearly ordered set consists of simply one path. For example, Fig. 7-1(*c*) is the diagram of such a set with five elements.



(*a*) (*b*) (*c*)

Fig. 7-1

EXAMPLE 7.4 A *partition* of a positive integer m is a set of positive integers whose sum is m. For instance, there are 7 partitions of $m = 5$ as follows:

5, 3-2, 2-2-1, 1-1-1-1-1, 4-1, 3-1-1, 2-1-1-1

We order the partitions of an integer m as follows. A partition P_1 precedes a partition P_2 if the integers in P_1 can be added to obtain the integers in P_2 or, equivalently, if the integers in P_2 can be further subdivided to obtain the integers in P_1. For example,

2-2-1 precedes 3-2 and 4-1

since $2 + 1 = 3$ and $2 + 2 = 4$. On the other hand, 3-1-1 and 2-2-1 are noncomparable.

Figure 7-2 gives the Hasse diagram of the partitions of $m = 5$.

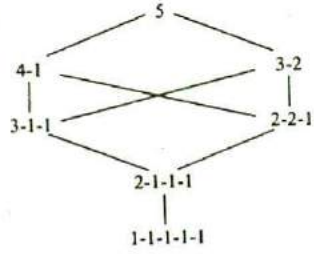


Fig. 7-2

7.5 MINIMAL AND MAXIMAL ELEMENTS, FIRST AND LAST ELEMENTS

Let S be a partially ordered set. An element $a \in S$ is called a *minimal* element of S if no element of S strictly precedes (is less than) a; that is, if

$$x \leq a \text{ implies } x = a$$

Similarly, an element $b \in S$ is called a *maximal* element of S if no element of S strictly succeeds (is greater than) b; that is, if

$$x \geq b \text{ implies } x = b$$

Geometrically speaking, a is a minimal element of S if no edge enters a (from below), and b is a maximal element of S if no edge leaves b (in an upward direction). We note that S can have more than one minimal and more than one maximal element.

If S is infinite, then S may have no minimal and no maximal element. For instance, the set $\mathbf{Z}$ of integers with the usual order $\leq$ has no minimal and no maximal element. On the other hand, if S is finite, then S has at least one minimal element and one maximal element.

An element $a \in S$ is called a *first* element of S if

$$a \leq x$$

for every $x \in S$, that is, if a precedes every other element in S. Similarly, an element $b \in S$ is called a *last* element of S if

$$y \leq b$$

for every $y \in S$, that is, if b succeeds every other element in S. We note that S can have at most one first element which must be a minimal element of S, and S can have at most one last element which must be a maximal element of S. Generally speaking, S may have neither a first nor a last element, even when S is finite.

Now suppose that S is a linearly ordered set. If S has a minimal element, then it must also be a first element; and if S has a maximal element, then it must also be a last element. In particular, if S is a finite linearly ordered set, then S has both a first element and a last element.

EXAMPLE 7.5 Consider the three partially ordered sets in Example 7.3 whose Hasse diagrams appear in Fig. 7-1.

(*a*) A has two maximal elements, 18 and 24, and neither is a last element. A has only one minimal element, 1, which is also a first element.

(*b*) B has two minimal elements, d and e, and neither is a first element. B has only one maximal element a, which is also a last element.

(*c*) The linearly ordered set $\{x, y, z, u, v\}$ has one minimal element, x, which is a first element, and one maximal element, v, which is a last element.

EXAMPLE 7.6

(*a*) Consider the set $\mathbf{P} = \{1, 2, 3, \ldots\}$ with the usual order $\leq$. Then 1 is a first and only minimal element. $\mathbf{P}$ has no last and no maximal element.

(*b*) Let A be any nonempty set and let $\mathscr{P}(A)$ be the power set of A ordered by set inclusion. Then the empty set $\varnothing$ is a first element of $\mathscr{P}(A)$ since $\varnothing \subseteq X$ for any set X. Moreover, A is a last element of $\mathscr{P}(A)$ since every set Y in $\mathscr{P}(A)$ is a subset of A, that is, $Y \subseteq A$.

(*c*) Let $S = \{a_1, a_2, \ldots, a_m\}$ be a finite linearly ordered set. Then S contains precisely one minimal element and precisely one maximal element, denoted respectively by

$$\min(a_1, a_2, \ldots, a_m) \quad \text{and} \quad \max(a_1, a_2, \ldots, a_m)$$

7.6 CONSISTENT ENUMERATION

Suppose S is a finite partially ordered set. Frequently we want to assign a positive integer to each element of S in such a way that the order is preserved. That is, we seek a function $f: S \to \mathbf{P}$ so that if $a < b$ then $f(a) < f(b)$. Such a function f is called a *consistent enumeration* of S. The fact that this can be done is the content of the following theorem.

Theorem 7.1: There exists a consistent enumeration for any finite partially ordered set S.

We prove this theorem in Problem 7.17. In fact, we prove that if S has n elements then there exists a consistent enumeration $f: S \to \{1, 2, \ldots, n\}$.

We emphasize that such an enumeration need not be unique. For example, the following are two such enumerations for the ordered set in Fig. 7-1(*b*):

(i) $f(d) = 1, \quad f(e) = 2, \quad f(b) = 3, \quad f(c) = 4, \quad f(a) = 5$

(ii) $g(e) = 1, \quad g(d) = 2, \quad g(c) = 3, \quad g(b) = 4, \quad g(a) = 5$

On the other hand, the linearly ordered set in Fig. 7-1(*c*) admits only one consistent enumeration if we map the set into $\{1, 2, 3, 4, 5\}$. Specifically, we must assign:

$$h(x) = 1, \quad h(y) = 2, \quad h(z) = 3, \quad h(u) = 4, \quad h(v) = 5$$

7.7 SUPREMUM AND INFIMUM

Let S be a partially ordered set, and let A be a subset of S. An element M in S is called an *upper bound* of A if M succeeds every element of A, that is, for every $x \in A$, we have

$$x \leq M$$

If an upper bound of A precedes every other upper bound of A, then it is called the *supremum* of A and it is denoted by

$$\sup(A)$$

We also write $\sup(a_1, \ldots, a_n)$ instead of $\sup(A)$ when A consists of the elements $a_1, \ldots, a_n$. We emphasize that there can be at most one $\sup(A)$; however, $\sup(A)$ may not exist.

Analogously, an element m in S is called a *lower bound* of a subset A if m precedes every element of A, that is, for every $y \in A$, we have

$$m \leq y$$

If a lower bound of A succeeds every other lower bound of A, then it is called the *infimum* of A and it is denoted by

$$\inf(A)$$

We also write $\inf(a_1, \ldots, a_n)$ instead of $\inf(A)$ when A consists of the elements $a_1, \ldots, a_n$. Similarly, there can be at most one $\inf(A)$ although $\inf(A)$ may not exist.

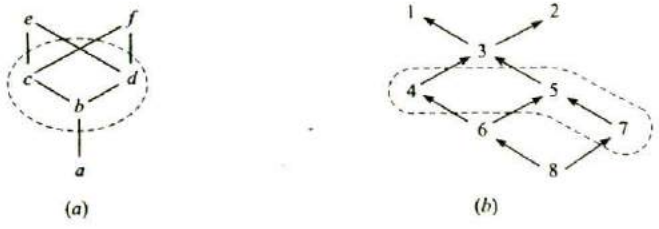
Some texts use the term *least upper bound* instead of supremum and then write $\text{lub}(A)$ instead of $\sup(A)$, and use the term *greatest lower bound* instead of infimum and then write $\text{glb}(A)$ instead of $\inf(A)$.

If A has an upper bound we say A is *bounded above*, and if A has a lower bound we say A is *bounded below*. In particular, A is *bounded* if A has an upper and lower bound.

EXAMPLE 7.7

(*a*) Let $S = \{a, b, c, d, e, f\}$ be ordered as pictured in Fig. 7-3(*a*), and let $A = \{b, c, d\}$. The upper bounds of A are e and f since only e and f succeed every element in A. The lower bounds of A are a and b since only a and b precede every element of A. Note e and f are noncomparable; hence $\sup(A)$ does not exist. However, b also succeeds a, hence $\inf(A) = b$. Observe that $\inf(A) = b$ does belong to A.

(*b*) Let $S = \{1, 2, 3, \ldots, 8\}$ be ordered as pictured in Fig. 7-3(*b*), and let $A = \{4, 5, 7\}$. The upper bounds of A are 1, 2, and 3, and the only lower bound is 8. Note that 7 is not a lower bound since 7 does not precede 4. Here $\sup(A) = 3$ since 3 precedes the other upper bounds 1 and 2, and $\inf(A) = 8$ since 8 is the only lower bound. Observe that neither $\inf(A) = 8$ nor $\sup(A) = 3$ belongs to A.



(*a*) (*b*)

Fig. 7-3

(*c*) Consider the set $\mathbf{Q}$ of rational numbers, and its subset

$$B = \{x \in \mathbf{Q} : x > 0 \text{ and } 2 < x^2 < 3\}$$

that is, B consists of those rational numbers which lie between $\sqrt{2}$ and $\sqrt{3}$ on the real line $\mathbf{R}$. Then B has an infinite number of upper and lower bounds, but $\inf(B)$ and $\sup(B)$ do not exist. In other words, B has no least upper bound and no greatest lower bound. Note that $\sqrt{2}$ and $\sqrt{3}$ do not belong to $\mathbf{Q}$ and cannot be considered as upper or lower bounds of B.

The above Example 7.7(*c*) points out one of the main differences between the real numbers **R** and the rational numbers **Q**. That is:

> **Completeness Axiom of the Real Numbers R:**
> Let A be a nonempty subset of **R** and suppose A has an upper bound. Then A has a least upper bound, that is, $\sup(A)$ exists.

Existence of $\sup(a, b)$ and $\inf(a, b)$

Let S be an ordered set and let $a, b \in S$. If S is linearly ordered, then $\sup(a, b)$ and $\inf(a, b)$ clearly exist. Specifically, if $a \leq b$, then $\sup(a, b) = b$ and $\inf(a, b) = a$. On the other hand, if S is an arbitrary ordered set, then $\sup(a, b)$ and $\inf(a, b)$ need not exist. However, there are important examples of nonlinearly ordered sets where $\sup(a, b)$ and $\inf(a, b)$ do exist for every a, b in the set.

EXAMPLE 7.8

(*a*) Consider the set $\mathbf{P} = \{1, 2, 3, \ldots\}$. The *greatest common divisor* of a and b in **P**, denoted by

$$\gcd(a, b)$$

is the largest integer which divides a and b. The *least common multiple* of a and b, denoted by

$$\operatorname{lcm}(a, b)$$

is the smallest integer divisible by both a and b.

An important theorem in number theory says that every common divisor of a and b divides $\gcd(a, b)$. Also, one can prove that $\operatorname{lcm}(a, b)$ divides every multiple of a and b.

Suppose **P** is ordered by divisibility. Then

$$\gcd(a, b) = \inf(a, b) \qquad \text{and} \qquad \operatorname{lcm}(a, b) = \sup(a, b)$$

In other words, $\inf(a, b)$ and $\sup(a, b)$ do exist for any pair a, b of elements of **P** ordered by divisibility.

(*b*) For any positive integer m, we will let $\mathbf{D}_m$ denote the set of divisors of m ordered by divisibility. The Hasse diagram of

$$\mathbf{D}_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

appears in Fig. 7-4. Again, $\inf(a, b) = \gcd(a, b)$ and $\sup(a, b) = \operatorname{lcm}(a, b)$ exist for any pair $a, b \in \mathbf{D}_m$.

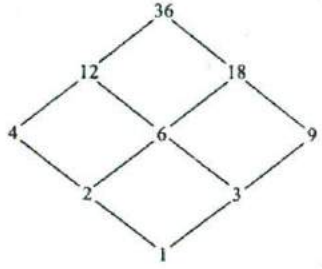


Fig. 7-4

(*c*) Let S be a nonempty set with at least two elements, and let $\mathscr{P}(S)$ be the power set of S ordered by set inclusion. Let A and B be any two elements of $\mathscr{P}(A)$, that is, let A and B be subsets of S. Then $\sup(A, B)$ and $\inf(A, B)$ do exist. Specifically, $\sup(A, B) = A \cup B$ and $\inf(A, B) = A \cap B$.

7.8 ISOMORPHIC (SIMILAR) ORDERED SETS

Suppose X and Y are partially ordered sets. A one-to-one (injective) function $f: X \to Y$ is called a *similarity mapping* from X into Y if f preserves the order relation, that is, if the following condition holds for any pair $a, b \in X$:

$$\boxed{a \leq b \text{ in } X \text{ if and only if } f(a) \leq f(b) \text{ in } Y}$$

The above condition is equivalent to the following two conditions:

(1) If $a \leq b$ then $f(a) \leq f(b)$.
(2) If $a \| b$ (noncomparable), then $f(a) \| f(b)$.

Accordingly, if the underlying sets X and Y are both linearly ordered, then only (1) is needed for f to be a similarity mapping.

Two ordered sets X and Y are said to be *order-isomorphic* or *isomorphic* or *similar*, written

$$X \simeq Y$$

if there exists a one-to-one correspondence (bijective mapping) $f: X \to Y$ which preserves the order relations, i.e., which is a similarity mapping. Such a function f is then called an *order-isomorphism* or *isomorphism* from X onto Y or an *order-isomorphism* between X and Y.

EXAMPLE 7.9

(*a*) Suppose $S = \{a, b, c, d\}$ is ordered by the diagram in Fig. 7-5(*a*) and suppose $T = \{1, 2, 6, 8\}$ is ordered by divisibility. Figure 7-5(*b*) is the Hasse diagram of the ordered set T. Then $S \simeq T$. In particular, the following function $f: S \to T$ is an isomorphism between S and T:

$$f(a) = 6, \quad f(b) = 8, \quad f(c) = 2, \quad f(d) = 1$$

We note that the following function $g: S \to T$ is another isomorphism between S and T:

$$g(a) = 8, \quad g(b) = 6, \quad g(c) = 2, \quad g(d) = 1$$

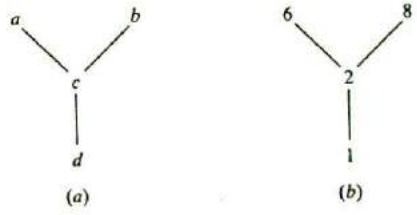


Fig. 7-5

(*b*) The set of positive integers $\mathbf{P} = \{1, 2, 3, \ldots\}$ is order-isomorphic to the set of even positive integers $E = \{2, 4, 6, \ldots\}$ since the function $f: \mathbf{P} \to E$ defined by $f(x) = 2x$ is an isomorphism between $\mathbf{P}$ and E.

(*c*) Consider the usual ordering $\leq$ of the positive integers $\mathbf{P} = \{1, 2, 3, \ldots\}$ and the negative integers $A = \{-1, -2, -3, \ldots\}$. Then $\mathbf{P}$ is not order-isomorphic to A. For if $f: \mathbf{P} \to A$ is an isomorphism then, for every $n \in \mathbf{P}$,

$$1 \leq n \quad \text{should imply} \quad f(1) \leq f(n)$$

for every $f(n) \in A$. Since A has no first element, f cannot exist.

The following theorems follow directly from the definition of order-isomorphic sets.

Theorem 7.2: Suppose S is linearly ordered and $T \simeq S$. Then T is linearly ordered.

Theorem 7.3: Suppose $f: S \to T$ is an order-isomorphism between ordered sets S and T. Then $a \in S$ is a first, last, minimal, or maximal element of S if and only if $f(a)$ is, respectively, a first, last, minimal, or maximal element of T.

Theorem 7.4: If S is order-isomorphic to T, then S is equipotent to T; that is, if $S \simeq T$ then $|S| = |T|$.

Example 7.9(*c*) shows that the converse of the above theorem is not true. That is, equipotent ordered sets need not be order-isomorphic.

Theorem 7.5: The relation of order-isomorphism between ordered sets is an equivalence relation. That is:

(i) $S \simeq S$, for any ordered set S.

(ii) If $S \simeq T$, then $T \simeq S$.

(iii) If $S \simeq T$ and $T \simeq U$, then $S \simeq U$.

7.9 ORDER TYPES OF LINEARLY ORDERED SETS

Consider a collection $\mathscr{S}$ of linearly ordered sets. Each set A in $\mathscr{S}$ is assigned a symbol in such a way that two linearly ordered sets A and B in $\mathscr{S}$ are assigned the same symbol if and only if the sets are order-isomorphic. This symbol is called the *order type* of the sets. (One may view the order type as the equivalence class of all order-isomorphic sets in $\mathscr{S}$.) We emphasize that order type is only defined for linearly ordered sets, not ordered sets in general.

The order types of the following familiar sets (with the usual order) follow:

ω = order type of the set $\mathbf{P}$ of positive integers

π = order type of the set $\mathbf{Z}$ of integers

η = order type of the set $\mathbf{Q}$ of rational numbers

Moreover, if ζ is the order type of a linearly ordered set S, then ζ^* will denote the order type of S with the inverse order.

EXAMPLE 7-10

(*a*) Consider the following sets:

$$\mathbf{P} = \{1, 2, 3, \ldots\} \text{ of positive integers,}$$
$$E = \{2, 4, 6, \ldots\} \text{ of even positive integers,}$$
$$A = \{\ldots, -3, -2, -1\} \text{ of negative integers.}$$

The order type of set E is ω since E is order-isomorphic to $\mathbf{P}$, but the order type of the set A is not ω since A is not order-isomorphic to $\mathbf{P}$. However, the order type of A is ω^* since A is order-isomorphic to $\mathbf{P}$ with the inverse order.

(*b*) $\mathbf{P} = \{1, 2, 3, \ldots\}$ with the usual order is not order-isomorphic to $\mathbf{P}$ with the inverse order; hence $\omega \neq \omega^*$. On the other hand,

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

with the usual order is order-isomorphic to $\mathbf{Z}$ with the inverse order; hence $\pi = \pi^*$.

7.10 LATTICES

Let L be a nonempty set closed under two binary operations called *meet* and *join*, denoted respectively by $\wedge$ and $\vee$. Then L is called a *lattice* if the following axioms hold where a, b, c are any elements in L:

$[\mathbf{L}_1]$ ***Commutative law***:
$(1a)\ a \wedge b = b \wedge a$ $\qquad$ $(1b)\ a \vee b = b \vee a$

$[\mathbf{L}_2]$ ***Associative law***:
$(2a)\ (a \wedge b) \wedge c = a \wedge (b \wedge c)$ $\qquad$ $(2b)\ (a \vee b) \vee c = a \vee (b \vee c)$

$[\mathbf{L}_3]$ ***Absorption law***:
$(3a)\ a \wedge (a \vee b) = a$ $\qquad$ $(3b)\ a \vee (a \wedge b) = a$

We will sometimes denote the lattice by $(L, \wedge, \vee)$ when we want to show which operations are involved.

Duality and the Idempotent Law

The *dual* of any statement in a lattice $(L, \wedge, \vee)$ is defined to be the statement that is obtained by interchanging $\wedge$ and $\vee$. For example, the dual of

$$a \wedge (b \vee a) = a \vee a \qquad \text{is} \qquad a \vee (b \wedge a) = a \wedge a$$

Notice that the dual of each axiom of a lattice is also an axiom. Accordingly, the principle of duality holds; that is:

Theorem 7.6 (Principle of Duality): The dual of any theorem in a lattice is also a theorem.

This follows from the fact that the dual theorem can be proven by using the dual of each step of the proof of the original theorem.

An important property of lattices follows directly from the absorption laws.

Theorem 7.7 (Idempotent Law): (i) $a \wedge a = a$, (ii) $a \vee a = a$.

The proof of (i) requires only two lines:

$$\begin{aligned} a \wedge a &= a \wedge (a \vee (a \wedge b)) && \text{(using } (3b)\text{)} \\ &= a && \text{(using } (3a)\text{)} \end{aligned}$$

The proof of (ii) follows from the above principle of duality (or can be proved in a similar manner).

Lattices and Order

Given a lattice L, we can define a partial order on L as follows:

$$a \leq b \qquad \text{if} \qquad a \wedge b = a$$

Analogously, we could define

$$a \leq b \qquad \text{if} \qquad a \vee b = b$$

We state these results in a theorem.

Theorem 7.8: Let L be a lattice. Then:

(i) $a \wedge b = a$ if and only if $a \vee b = b$.

(ii) The relation $a \leq b$ (defined by $a \wedge b = a$ or $a \vee b = b$) is a partial order on L.

Now that we have a partial order on any lattice L, we can picture L by a diagram as was done for partially ordered sets in general.

EXAMPLE 7.11 Let C be a collection of sets closed under intersection and union. Then $(C, \cap, \cup)$ is a lattice. In this lattice, the partial order relation is the same as the set inclusion relation. Figure 7-6 shows the diagram of the lattice L of all subsets of $\{a, b, c\}$.

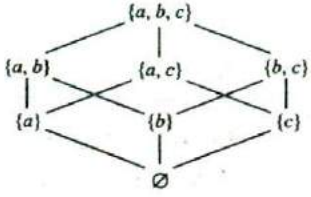


Fig. 7-6

We have shown how to define a partial order on a lattice L. The next theorem tells us when we can define a lattice on a partially ordered set P such that the lattice will give back the original order on P.

Theorem 7.9: Let P be a partially ordered set such that the $\inf(a, b)$ and $\sup(a, b)$ exist for any a, b in P. Letting

$$a \wedge b = \inf(a, b) \qquad \text{and} \qquad a \vee b = \sup(a, b)$$

we have that $(P, \wedge, \vee)$ is a lattice. Furthermore, the partial order on P induced by the lattice is the same as the original partial order on P.

The converse of the above theorem is also true. That is, let L be a lattice and let $\leq$ be the induced partial order on L. Then $\inf(a, b)$ and $\sup(a, b)$ exist for any pair a, b in L and the lattice obtained from the ordered set $(L, \leq)$ is the original lattice. Accordingly, we have the following:

Alternate Definition: A lattice is a partially ordered set in which

$$a \wedge b = \inf(a, b) \qquad \text{and} \qquad a \vee b = \sup(a, b)$$

exist for any pair of elements a and b.

We note first that any linearly ordered set is a lattice since $\inf(a, b) = a$ and $\sup(a, b) = b$ whenever $a \leq b$. By Example 7.8, the positive integers $\mathbf{P}$ and the set $\mathbf{D}_m$ of divisors of m are lattices under the relation of divisibility.

Sublattices, Isomorphic Lattices

Suppose M is a nonempty subset of a lattice L. We say M is a *sublattice* of L if M itself is a lattice (with respect to the operations of L). We note that M is a sublattice of L if and only if M is closed under the operations of $\wedge$ and $\vee$ of L. For example, the set $\mathbf{D}_m$ of divisors of m is a sublattice of the positive integers N under divisibility.

Two lattices L and L' are said to be *isomorphic* if there is a one-to-one correspondence $f: L \to L'$ such that

$$f(a \wedge b) = f(a) \wedge f(b) \qquad \text{and} \qquad f(a \vee b) = f(a) \vee f(b)$$

for any elements a, b in L.

7.11 BOUNDED, DISTRIBUTIVE, COMPLEMENTED LATTICES

This section discusses a number of different kinds of lattices, bounded, distributive, and complemented lattices. We also discuss a number of special kinds of elements in a lattice, join irreducible elements, atoms, and complements.

Bounded Lattices

A lattice L is said to have a *lower bound* 0 if for any element x in L we have $0 \precsim x$. Analogously, L is said to have an *upper bound* I if for any x in L we have $x \precsim I$. We say L is *bounded* if L has both a lower bound 0 and an upper bound I. In such a lattice we have the identities

$$a \vee I = I, \qquad a \wedge I = a, \qquad a \vee 0 = a, \qquad a \wedge 0 = 0$$

for any element a in L.

The nonnegative integers with the usual ordering,

$$0 < 1 < 2 < 3 < 4 < \dots$$

have 0 as a lower bound but have no upper bound. On the other hand, the lattice $P(\mathbf{U})$ of all subsets of any universal set $\mathbf{U}$ is a bounded lattice with $\mathbf{U}$ as an upper bound and the empty set $\varnothing$ as a lower bound.

Suppose $L = \{a_1, a_2, \dots, a_n\}$ is a finite lattice. Then

$$a_1 \vee a_2 \vee \cdots \vee a_n \quad \text{and} \quad a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

are upper and lower bounds for L, respectively. Thus we have

Theorem 7.10: Every finite lattice L is bounded.

Distributive Lattices

A lattice L is said to be *distributive* if for any elements a, b, c in L we have the following:

[L_4] ***Distributive law***:

$$(4a)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \qquad (4b)\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Otherwise, L is said to be *nondistributive*. We note that by the principle of duality the condition (4a) holds if and only if (4b) holds

Figure 7-7(a) is a nondistributive lattice since

$$a \vee (b \wedge c) = a \vee 0 = a$$

but

$$(a \vee b) \wedge (a \vee c) = I \wedge c = c$$

Figure 7-7(b) is also a nondistributive lattice. In fact, we have the following characterization of such lattices.

Theorem 7.11: A lattice L is nondistributive if and only if it contains a sublattice isomorphic to Fig. 7-7(a) or (b).

The proof of this theorem lies beyond the scope of this text.

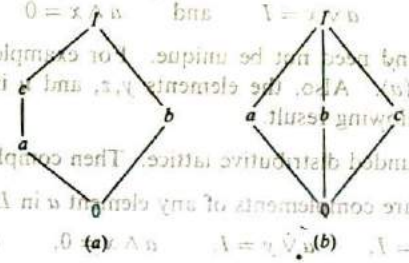


Fig. 7-7

Join-Irreducible Elements, Atoms

Let L be a lattice with a lower bound 0. An element a in L is said to be *join irreducible* if $a = x \vee y$ implies $a = x$ or $a = y$. (Prime numbers under multiplication have this property, i.e., if $p = ab$ then $p = a$

or $p = b$ where p is prime.) Clearly 0 is join irreducible. If a has at least two immediate predecessors, say b_1 and b_2 as in Fig. 7-8(a), then $a = b_1 \vee b_2$, and so a is not join irreducible. On the other hand, if a has a unique immediate predecessor c, then $a \neq \sup(b_1, b_2) = b_1 \vee b_2$ for any other elements b_1 and b_2 because c would lie between the b's and a as in Fig. 7-8(b). In other words, $a \neq 0$ is join irreducible if and only if a has a unique immediate predecessor. Those elements which immediately succeed 0, called *atoms*, are join irreducible. However, lattices can have other join-irreducible elements. For example, the element c in Fig. 7-8(a) is not an atom but is join irreducible since a is its only immediate predecessor.

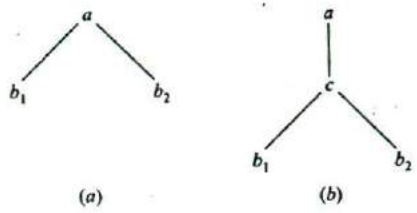


Fig. 7-8

If an element a in a finite lattice L is not join irreducible, then we can write $a = b_1 \vee b_2$. Then we can write b_1 and b_2 as the join of other elements if they are not join irreducible; and so on. Since L is finite we finally have

$$a = d_1 \vee d_2 \vee \cdots \vee d_n$$

where the d's are join irreducible. If d_i precedes d_j then $d_i \vee d_j = d_j$; so we can delete the d_i from the expression. In other words, we can assume that the d's are *irredundant*, i.e., no d precedes any other d. We emphasize that such an expression need not be unique, e.g., $I = a \vee b$ and $I = b \vee c$ in both lattices in Fig. 7-7(b). We now state the main theorem of this section (proved in Problem 7.39).

Theorem 7.12: Let L be a finite distributive lattice. Then every a in L can be written uniquely (except for order) as the join of irredundant join-irreducible elements.

Actually this theorem can be generalized to lattices with *finite length*, i.e., where all linearly ordered subsets are finite. (Problem 7.34 gives an infinite lattice with finite length.)

Complements

Let L be a bounded lattice with lower bound 0 and upper bound I. Let a be an element of L. An element x in L is called a *complement* of a if

$$a \vee x = I \qquad \text{and} \qquad a \wedge x = 0$$

Complements need not exist and need not be unique. For example, the elements a and c are both complements of b in Fig. 7-7(a). Also, the elements y, z, and u in the chain in Fig. 7-1 have no complements. We have the following result.

Theorem 7.13: Let L be a bounded distributive lattice. Then complements are unique if they exist.

Proof: Suppose x and y are complements of any element a in L. Then

$$a \vee x = I, \qquad a \vee y = I, \qquad a \wedge x = 0, \qquad a \wedge y = 0$$

Using distributivity,

$$x = x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = I \wedge (x \vee y) = x \vee y$$

Similarly,

$$y = y \vee 0 = y \vee (a \wedge x) = (y \vee a) \wedge (y \vee x) = I \wedge (y \vee x) = y \vee x$$

Thus $x = x \vee y = y \vee x = y$ and the theorem is proved.

Complemented Lattices

A lattice L is said to be *complemented* if L is bounded and every element in L has a complement. Figure 7-7(b) shows a complemented lattice where complements are not unique. On the other hand, the lattice $P(\mathrm{U})$ of all subsets of a universal set U is complemented, and each subset A of U has the unique complement $A^c = \mathrm{U} \backslash A$.

Theorem 7.14: Let L be a complemented lattice with unique complements. Then the join-irreducible elements of L, other than 0, are its atoms.

Combining this theorem and Theorems 7.12 and 7.13 we get an important result.

Theorem 7.15: Let L be a finite complemented distributive lattice. Then every element a in L is the join of a unique set of atoms.

Remark: Some texts define a lattice L to be complemented if each a in L has a unique complement. Theorem 7.14 is then stated differently.

Solved Problems

ORDERED SETS AND SUBSETS

7.1. Suppose the set $\mathbf{P} = \{1, 2, 3, \ldots\}$ of positive integers is ordered by divisibility. Insert the correct symbol, $<$, $>$, or $\|$ (not comparable), between each pair of numbers:

(a) 2 ____ 8, (b) 18 ____ 24, (c) 9 ____ 3, (d) 5 ____ 15.

(a) Since 2 divides 8, 2 precedes 8; hence $2 < 8$.

(b) 18 does not divide 24, and 24 does not divide 18; hence $18 \| 24$.

(c) Since 9 is divisible by 3, $9 > 3$.

(d) Since 5 divides 15, $5 < 15$.

7.2. Let $\mathbf{P} = \{1, 2, 3, \ldots\}$ be ordered by divisibility. State whether each of the following is a chain (linearly ordered subset) in $\mathbf{P}$.

(a) $A = \{24, 2, 6\}$ (c) $C = \{2, 8, 32, 4\}$ (e) $E = \{15, 5, 30\}$

(b) $B = \{3, 15, 5\}$ (d) $D = \{7\}$ (f) $\mathbf{P} = \{1, 2, 3, \ldots\}$

(a) Since 2 divides 6 which divides 24, A is a chain in $\mathbf{P}$.

(b) Since 3 and 5 are noncomparable, B is not a chain in $\mathbf{P}$.

(c) C is a chain in $\mathbf{P}$ since $2 < 4 < 8 < 32$, that is, $2|4|8|32$ where $|$ means divides.

(d) Any set consisting of one element is linearly ordered; hence D is a chain in $\mathbf{P}$.

(e) Here $5 < 15 < 30$; hence E is a chain in $\mathbf{P}$.

(f) $\mathbf{P}$ is not linearly ordered, e.g., 2 and 3 are noncomparable; hence $\mathbf{P}$ itself is not a chain in $\mathbf{P}$.

7.3. Let $A = \{1, 2, 3, 4, 5\}$ be ordered by the Hasse diagram in Fig. 7-9. Insert the correct symbol, $<$, $>$, or $\|$ (not comparable), between each pair of elements:

(*a*) 1 ___ 5; (*b*) 2 ___ 3; (*c*) 4 ___ 1; (*d*) 3 ___ 4

(*a*) Since there is a "path" (edges slanting upward) from 5 to 3 to 1, 5 precedes 1; hence $1 > 5$.

(*b*) There is no path from 2 to 3, or vice versa; hence $2 \| 3$.

(*c*) There is a path from 4 to 2 to 1; hence $4 < 1$.

(*d*) Neither $3 < 4$ nor $4 < 3$; hence $3 \| 4$.

7.4. Consider the ordered set A in Fig. 7-9.

(*a*) Find all minimal and maximal elements of A.

(*b*) Does A have a first element or a last element?

(*a*) No element strictly precedes 4 or 5, so 4 and 5 are minimal elements of A. No element strictly succeeds 1, so 1 is a maximal element of A.

(*b*) A has no first element. Although 4 and 5 are minimal elements of A, neither precedes the other. However, 1 is a last element of A since 1 succeeds every element of A.

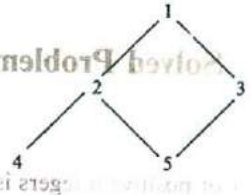


Fig. 7-9

7.5. Consider the ordered set A in Fig. 7-9. For each $a \in A$, let $p(a)$ denote the set of predecessors of a, that is,

$$p(a) = \{x : x \leq a\}$$

Let $p(A)$ denote the collection of all predecessor sets of A, and let $p(A)$ be ordered by set inclusion. Draw the Hasse diagram of $p(A)$.

The elements of $p(A)$ follow:

$$p(1) = \{1, 2, 3, 4, 5\}, \quad p(2) = \{2, 4, 5\}, \quad p(3) = \{3, 5\}, \quad p(4) = \{4\}, \quad p(5) = \{5\}$$

Figure 7-10 gives the Hasse diagram of $p(A)$ ordered by set inclusion. [Observe that the diagrams of A and $p(A)$ are identical except for the labeling of the vertices.]

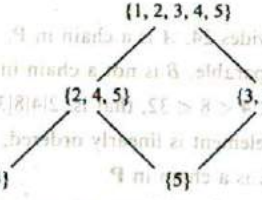


Fig. 7-10

7.6. Consider the ordered set A in Fig. 7-9. Let $\mathcal{L}(A)$ denote the collection of all chains (linearly ordered subsets) in A with 2 or more elements, and let $L(A)$ be ordered by set inclusion. Draw the Hasse diagram of $L(A)$.

The elements of $L(A)$ are as follows:

$$\{1,2,4\}, \{1,2,5\}, \{1,3,5\}, \{1,2\}, \{1,4\}, \{1,3\}, \{1,5\}, \{2,4\}, \{2,5\}, \{3,5\}$$

(Note $\{2,5\}$ and $\{3,4\}$ are not linearly ordered, and there are no chains with four or more elements.) The diagram of $L(A)$ appears in Fig. 7-11.

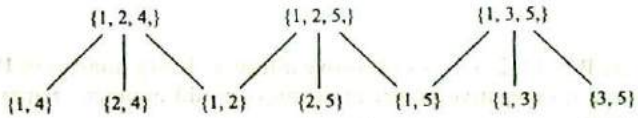


Fig. 7-11

7.7. Prerequisites in college is a familiar partial ordering of available classes. Define $A < B$ if class A is a prerequisite for class B. Let C be the set of mathematics classes and their prerequisites given in Fig. 7-12(a).

(a) Draw the Hasse diagram for the partial ordering of these classes.

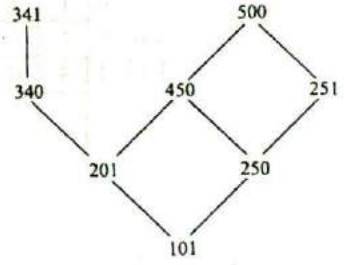
(b) Find all minimal and maximal elements of C.

(c) Does C have a first element or a last element?

(a) Math 101 must be on the bottom of the diagram since it is the only course with no prerequisites. Since Math 201 and Math 250 only require Math 101, we have Math 101 << Math 201 and we have Math 101 << Math 250; hence draw a line slanting upward from Math 101 to Math 201 and one from Math 101 to Math 250. Continuing this process, we obtain the Hasse diagram in Fig. 7-12(b).

Class	Prerequisites
Math 101	None
Math 201	Math 101
Math 250	Math 101
Math 251	Math 250
Math 340	Math 201
Math 341	Math 340
Math 450	Math 201, Math 250
Math 500	Math 450, Math 251

(a)



(b)

Fig. 7-12

(b) No element strictly precedes Math 101 so Math 101 is a minimal element of C. No element strictly succeeds Math 341 or Math 500, so each is a maximal element of C.

(c) Math 101 is a first element of C since it precedes every other element of C. However, C has no last element. Although Math 341 and Math 500 are maximal elements, neither is a last element since neither precedes the other.

7.8. Consider the set $\mathbf{Z}$ of integers. Define $a R b$ by $b = a^r$ for some positive integer r. Show that R is a partial order on $\mathbf{Z}$, that is, show that R is (a) reflexive, (b) antisymmetric, and (c) transitive.

(a) R is reflexive since $a = a^1$.

(b) Suppose $a R b$ and $b R a$, say $b = a^r$ and $a = b^s$. Then $a = (a^r)^s = a^{rs}$. There are three possibilities: (i) $rs = 1$, (ii) $a = 1$, and (iii) $a = -1$. If $rs = 1$, then $r = 1$ and $s = 1$ and so $a = b$. If $a = 1$, then $b = 1^r = 1 = a$, and, similarly, if $b = 1$, then $a = 1$. Lastly, if $a = -1$, then $b = -1$ (since $b \neq 1$) and so $a = b$. In all three cases, $a = b$. Thus R is antisymmetric.

(c) Suppose $a R b$ and $b R c$, say $b = a^r$ and $c = b^s$. Then $c = (a^r)^s = a^{rs}$ and hence $a R c$. Hence R is transitive.

7.9. Consider the set $\mathbf{P} = \{1, 2, 3, \ldots\}$ of positive integers. Every number in $\mathbf{P}$ can be written uniquely as a product of a nonnegative power of 2 times an odd number. Suppose a and a' are positive integers such that

$$a = 2^r(2s + 1) \qquad \text{and} \qquad a' = 2^{r'}(2s' + 1)$$

where r and s are nonnegative integers. We define:

$$a < a' \begin{cases} \text{if } r < r' \\ \text{or if } r = r' \text{ but } s < s' \end{cases}$$

Insert the correct symbol, $<$ or $>$, between each of the following pairs of numbers:

(a) 5 ____ 14, (b) 6 ____ 9, (c) 26 ____ 12, (d) 20 ____ 30

The elements of $\mathbf{P}$ can be listed as in Fig. 7-13. The first row consists of the odd numbers, the second row of 2 times the odd numbers, the third row of $2^2 = 4$ times the odd numbers, and so on. Then $a < a'$ if a is in a higher row than a', or if a and a' are in the same row but a comes before a' in the row. Thus:

(a) $5 < 14$, (b) $6 > 9$, (c) $26 < 12$, (d) $20 > 30$.

r \ s	0	1	2	3	4	5	6	7	
0	1	3	5	7	9	11	13	15	...
1	2	6	10	14	18	22	26	30	...
2	4	12	20	28	36	44	52	60	...
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Fig. 7-13

7.10. Suppose $<$ is a quasi-order on a set S. Define:

$$a \leq b \qquad \text{if} \qquad a < b \qquad \text{or} \qquad a = b$$

Show that $a \leq b$ is a partial order on S.

We want to show that $\leq$ is (a) reflexive, (b) antisymmetric, and (c) transitive.

(a) Since $a = a$, we have $a \leq a$. Hence $\leq$ is reflexive.

(b) Suppose $a \leq b$ and $b \leq a$. Then either $a = b$ or else $a < b$ and $b < a$. Suppose $a < b$ and $b < a$. By transitivity of $<$, we have $a < a$. This contradicts the fact that $<$ is irreflexive. Thus $a = b$ and $\leq$ is antisymmetric.

(c) Suppose $a \leq b$ and $b \leq c$. There are four cases.

(1) Suppose $a = b$ and $b = c$. Then $a = c$ and $a \leq c$.

(2) Suppose $a = b$ and $b < c$. Then $a < c$ and so $a \leq c$.

(3) Suppose $a < b$ and $b = c$. Then $a < c$ and so $a \leq c$.

(4) Suppose $a < b$ and $b < c$. Since $<$ is transitive, $a < c$. Hence $a \leq c$.

In each case, $a \leq c$; hence $\leq$ is transitive.

SET CONSTRUCTIONS AND ORDER

7.11. Suppose $\mathbf{P}$ has the usual order $\leq$. Consider the following pairs of elements of $\mathbf{P}^2 = \mathbf{P} \times \mathbf{P}$:

(a) (5, 7) ___ (7, 1) (c) (5, 5) ___ (4, 8) (e) (7, 9) ___ (4, 1)

(b) (4, 6) ___ (4, 2) (d) (1, 3) ___ (1, 7) (f) (7, 9) ___ (8, 2)

Insert the correct symbol, $<$, $>$, or $\|$ (not comparable), between each of the above pairs of elements of $\mathbf{P} \times \mathbf{P}$ when $\mathbf{P}^2$ is given (1) product order, (2) lexicographical order.

(1) Here $(a,b) \leq (a',b')$ provided $a \leq a'$ and $b \leq b'$. Hence $(a,b) < (a',b')$ if $a < a'$ and $b \leq b'$ or if $a \leq a'$ and $b < b'$. Thus:

(a) $\|$ since $5 < 7$ but $7 > 1$ (c) $\|$ since $5 > 4$ and $5 < 8$ (e) $>$ since $7 > 4$ and $9 > 1$

(b) $>$ since $4 \geq 4$ and $6 > 2$ (d) $<$ since $1 \leq 1$ and $3 < 7$ (f) $\|$ since $7 < 8$ and $9 > 2$

(2) Here $(a,b) < (a',b')$ if $a < a'$ or if $a = a'$ but $b < b'$. Thus:

(a) $<$ since $5 < 7$. (c) $>$ since $5 > 4$ (e) $>$ since $7 > 4$

(b) $>$ since $4 = 4$ and $6 > 2$ (d) $<$ since $1 = 1$ but $3 < 7$ (f) $<$ since $7 < 8$

7.12. Suppose the English alphabet $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ is given the *usual (alphabetical) order*. Consider the following two-letter words (viewed as elements of $\mathbf{A} \times \mathbf{A}$):

(a) cx ___ at (c) cx ___ cz (e) cx ___ dx

(b) cx ___ by (d) cx ___ rs (f) cx ___ cs

Insert the correct symbol, $<$, $>$, or $\|$ (not comparable), between each of the above two-letter words when $\mathbf{A}^2 = \mathbf{A} \times \mathbf{A}$ is given (1) the product order, (2) the lexicographical order.

(1) (a) $>$ since $c > a$ and $x > t$ (c) $<$ since $c \leq c$ and $x < z$ (e) $<$ since $c < d$ and $x \leq x$

(b) $\|$ since $c > b$ but $x < y$ (d) $\|$ since $c < r$ but $x > s$ (f) $>$ since $c \geq c$ and $x > s$

(2) (a) $>$ since $c > a$ (c) $<$ since $c = c$ and $x < z$ (e) $<$ since $c < d$

(b) $<$ since $c > b$ (d) $<$ since $c < r$ (f) $>$ since $c = c$ and $x > s$

7.13. Consider the set $\mathbf{P} = \{1, 2, 3, \ldots\}$ with the usual order, and the English alphabet $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ with the usual alphabetical order. Suppose $S = \mathbf{P} \cup \mathbf{A}$ and $T = \mathbf{A} \cup \mathbf{P}$ are each given the concatenation order:

$$S = \{1, 2, 3, \ldots; a, b, \ldots, z\}, \qquad T = \{a, b, \ldots, z; 1, 2, 3, \ldots\}$$

(Here $\mathbf{P} < \mathbf{A}$ in S but $\mathbf{A} < \mathbf{P}$ in T.) (a) Insert the correct symbol, $<$ or $>$, between the pair "7 ___ y". (b) Which subsets of S and of T are chains? (c) Which elements in S and which elements in T have no immediate predecessors?

(a) We have $7 < y$ when $7, y \in S$, but $7 > y$ when $7, y \in T$.

(b) Since S and T are linearly ordered, every subset of S and of T are chains.

(c) In S, both 1 and a have no immediate predecessor. However, in T only a has no immediate predecessor.

7.14. Consider the English alphabet $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ with the *usual (alphabetical) order*. Recall that the Kleene closure $\mathbf{A}^*$ of $\mathbf{A}$ consists of all words in $\mathbf{A}$. Let L be the following subset of $\mathbf{A}^*$:

$$L = \{\text{went, forget, to, medicine, me, toast, melt, for, we, arm}\}$$

Sort (arrange in order) L where $\mathbf{A}^*$ is given (*a*) the short-lex (free semigroup) order, (*b*) the lexicographical order.

(*a*) First order the elements by length and then order them alphabetically to obtain:

me, to, we, arm, for, melt, went, toast, forget, medicine

(*b*) Use the usual alphabetical ordering to obtain:

arm, for, forget, me, medicine, melt, to, toast, we, went

7.15. Suppose A and B are ordered sets. Show that the product order on $A \times B$, defined by

$$(a, b) \precsim (c, d) \quad \text{if } a \leq c \text{ and } b \leq d$$

is a partial ordering of $A \times B$.

We want to show that $\precsim$ is (*a*) reflexive, (*b*) antisymmetric, and (*c*) transitive.

(*a*) Since $a = a$ and $b = b$, we have $a \leq a$ and $b \leq b$. Hence $(a, b) \precsim (a, b)$ and $\precsim$ is reflexive.

(*b*) Suppose $(a, b) \precsim (c, d)$ and $(c, d) \precsim (a, b)$. Then

$$a \leq c \text{ and } b \leq d \quad \text{and} \quad c \leq a \text{ and } d \leq b$$

Thus $a = c$ and $b = d$. Hence $(a, b) = (c, d)$ and $\precsim$ is antisymmetric.

(*c*) Suppose $(a, b) \precsim (c, d)$ and $(c, d) \precsim (e, f)$. Then

$$a \leq c \text{ and } b \leq d \quad \text{and} \quad c \leq e \text{ and } d \leq f$$

By transitivity of $\leq$, we have $a \leq e$ and $b \leq f$. Thus $(a, b) \precsim (e, f)$, and $\precsim$ is transitive.

CONSISTENT ENUMERATIONS

7.16. Let $S = \{a, b, c, d, e\}$ be ordered as in Fig. 7-14. Find all possible consistent enumerations $f: S \to \{1, 2, 3, 4, 5\}$.

Since a is the only minimal element $f(a) = 1$, and since e is the only maximal element $f(e) = 5$. Also $f(b) = 2$ since b is the only successor of a. The choices for c and d are $f(c) = 3$ and $f(d) = 4$ or vice versa. Thus there are two possible enumerations which follow:

$$f(a) = 1, \quad f(b) = 2, \quad f(c) = 3, \quad f(d) = 4, \quad f(e) = 5$$
$$f(a) = 1, \quad f(b) = 2, \quad f(c) = 4, \quad f(d) = 3, \quad f(e) = 5$$

We emphasize that we usually cannot recreate the original partial order from a given consistent enumeration.

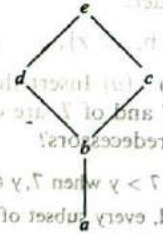


Fig. 7-14

7.17. Prove Theorem 7.1: Suppose S is a finite partially ordered set with n elements. Then there exists a consistent enumeration $f: S \to \{1, 2, \ldots, n\}$.

The proof is by induction on the number n of elements in S. Suppose $n = 1$, say $S = \{s\}$. Then $f(s) = 1$ is a consistent enumeration of S. Now suppose $n > 1$ and the theorem holds for ordered sets with less than n elements. Let a in S be a minimal element. [Such an element exists since S is finite.] Let $T = S \backslash \{a\}$. Then T is a finite poset with $n - 1$ elements and hence, by induction, T admits a consistent enumeration; say $g: T \to \{1, 2, \ldots, n-1\}$. Define $f: S \to \{1, 2, \ldots, n\}$ by

$$f(x) = \begin{cases} 1 & \text{if } x = a \\ g(x) + 1 & \text{if } x \neq a \end{cases}$$

Then f is the required consistent enumeration.

7.18. Suppose a student Ann wants to take all eight mathematics courses in Problem 7.7, but only one per semester.

(*a*) Which choice or choices does she have for her first and for her last (eighth) semester?

(*b*) Suppose she wants to take Math 250 in her first year (first or second semester) and Math 340 in her senior year (seventh or eighth semester). Find all possible ways that she can take the eight courses.

(*a*) By Fig. 7-12, Math 101 is the only minimal element and hence must be taken in the first semester, and Math 341 and 500 are the maximal elements and hence one of them must be taken in the last semester.

(*b*) Math 250 is not a minimal element and hence must be taken in the second semester, and Math 340 is not a maximal element so it must be taken in the seventh semester and Math 341 in the eighth semester. Also Math 500 must be taken in the sixth semester. The following give the three possible ways to take the eight courses:

[101, 250, 251, 201, 450, 500, 340, 341]
[101, 250, 201, 251, 450, 500, 340, 341]
[101, 250, 201, 450, 251, 500, 340, 341]

7.19. Suppose $\mathbf{P} = \{1, 2, 3, \ldots\}$ is ordered by divisibility "|". Find a consistent enumeration of $(\mathbf{P}, |)$ into $(\mathbf{P}, \leq)$.

The function $f: \mathbf{P} \to \mathbf{P}$ defined by $f(x) = x$ is a consistent enumeration since $a|b$ implies $a \leq b$.

7.20. Find a consistent enumeration of the real numbers $\mathbf{R}$ into $\mathbf{P}$.

Since $|\mathbf{R}| > |\mathbf{P}|$, there exists no one-to-one function from $\mathbf{R}$ into $\mathbf{P}$. Thus no consistent enumeration exists.

UPPER AND LOWER BOUNDS, SUPREMUM AND INFIMUM

7.21. Let $S = \{a, b, c, d, e, f, g\}$ be ordered as in Fig. 7-15, and let $X = \{c, d, e\}$.

(*a*) Find the upper and lower bounds of X.

(*b*) Identify $\sup(X)$, the supremum of X, and $\inf(X)$, the infimum of X, if either exists.

(*a*) The elements e, f and g succeed every element of X; hence e, f, and g are the upper bounds of X. The element a precedes every element of X; hence it is the lower bound of X. Note that b is not a lower bound since b does not precede c; in fact, b and c are not comparable.

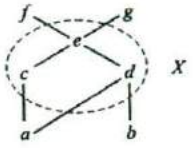


Fig. 7-15

(*b*) Since e precedes both f and g, we have $e = \sup(X)$. Likewise, since a precedes (trivially) every lower bound of X, we have $a = \inf(X)$. Note that $\sup(X)$ belongs to X but $\inf(X)$ does not belong to X.

7.22. Let $S = \{1, 2, 3, \ldots, 8\}$ be ordered as in Fig. 7-16, and let $A = \{2, 3, 6\}$.

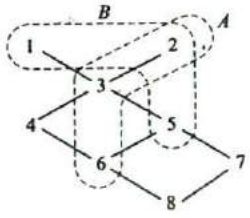


Fig. 7-16

(*a*) Find the upper and lower bounds of A.

(*b*) Identify $\sup(A)$ and $\inf(A)$ if either exists.

(*a*) The upper bound is 2, and the lower bounds are 6 and 8.

(*b*) Here $\sup(A) = 2$ and $\inf(A) = 6$.

7.23. Repeat Problem 7.22 for the subset $B = \{1, 2, 5\}$ of S.

(*a*) There is no upper bound for B since no element succeeds both 1 and 2. The lower bounds are 6, 7, 8.

(*b*) Trivially, $\sup(A)$ does not exist since there are no upper bounds. Although A has three lower bounds, $\inf(A)$ does not exist since no lower bound succeeds both 6 and 7.

7.24. Consider the set $\mathbf{Q}$ of rational numbers with the usual order $\leq$, and consider the subset D of $\mathbf{Q}$ defined by

$$D = \{x \in \mathbf{Q} : 8 < x^3 < 15\}$$

(*a*) Is D bounded above or below? (*b*) Do $\sup(D)$ and $\inf(D)$ exist?

(*a*) The subset D is bounded both above and below. For example, 1 is a lower bound and 100 an upper bound.

(*b*) $\sup(D)$ does not exist. Suppose, on the contrary, $\sup(D) = x$. Since $\sqrt[3]{15}$ is irrational, $x > \sqrt[3]{15}$. However, there exists a rational number y such that $\sqrt[3]{15} < y < x$. Thus y is also an upper bound for D. This contradicts the assumption that $x = \sup(D)$. On the other hand, $\inf(D)$ does exist. Specifically, $\inf(D) = 2$.

7.25. Let $\mathscr{S}$ be a collection of sets ordered by set inclusion. Let $\mathscr{A} = \{A_i : i \in I\}$ be a subcollection of $\mathscr{S}$. Let $B = \bigcup_i A_i$. (*a*) Suppose D is an upper bound of $\mathscr{A}$. Show that $B \subseteq D$. (*b*) Is B an upper bound of $\mathscr{A}$?

(*a*) Let $x \in B$. Then there exists $j \in I$ such that $x \in A_j$. Since D is an upper bound for $\mathscr{A}$, $A_j \subseteq D$. Hence $x \in D$. We have shown that $x \in B$ implies $x \in D$; hence $B \subseteq D$.

(*b*) Although $\mathscr{A} = \{A_i : i \in I\}$ is a subcollection of $\mathscr{S}$, it need not be true that $B = \bigcup_i A_i$ belongs to $\mathscr{S}$. Therefore, B is an upper bound if and only if B belongs to $\mathscr{S}$.

7.26. Given an example of a collection $\mathscr{S}$ of sets ordered by set inclusion, and a subcollection $\mathscr{A} = \{A_i : i \in I\}$ of $\mathscr{S}$ such that $B = \bigcup_i A_i$ is not an upper bound of $\mathscr{A}$.

Let $\mathscr{S}$ be the collection of all finite subsets of $\mathbf{P} = \{1, 2, 3, \ldots\}$ and let $\mathscr{A} = \{A_i\}$ be the subcollection of $\mathscr{S}$ consisting of sets with exactly two elements. Let $B = \bigcup_i A_i$. Then B has an infinite number of elements and hence B does not belong to $\mathscr{S}$. Thus B is not an upper bound of $\mathscr{A}$ (in $\mathscr{S}$).

ORDER-ISOMORPHIC SETS, SIMILARITY MAPPINGS

7.27. Suppose an ordered set A is order-isomorphic to an ordered set B and $f: A \to B$ is a similarity mapping. Are the following statements true or false?

(*a*) An element $a \in A$ immediately precedes an element $a' \in A$, that is, $a \prec a'$, if and only if $f(a) << f(a')$ in B.

(*b*) An element $a \in A$ has r immediate successors in A if and only if $f(a)$ has r immediate successors in B.

(*c*) An element $a \in A$ has r immediate predecessors in A if and only if $f(a)$ has r immediate predecessors in B.

All the statements are true; the order structure of A is the same as the order structure of B.

7.28. Let S be the ordered set in Fig. 7-14. Suppose $A = \{1, 2, 3, 4, 5\}$ is order-isomorphic to S and suppose the following is a similarity mapping from S onto A:

$$f = \{(a, 1), (b, 3), (c, 5), (d, 2), (e, 4)\}$$

Draw the Hasse diagram of A.

The similarity mapping f preserves the order structure of S and hence f may be viewed simply as a relabeling of the vertices in the diagram of S. Thus Fig. 7-17 shows the Hasse diagram of A.

Fig. 7-17

7.29. Let $S = \{1, 2, 3, 4, 5, 6\}$ be ordered as in Fig. 7-18(a).

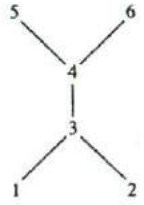
(a) Find the number n of similarity mappings $f: S \to S$.

(b) Is S order-isomorphic to S with the inverse ordering?

(a) Since 1 and 2 are the minimal elements, there are only two possibilities for $f(1)$ and $f(2)$; that is, $f(1) = 1$ and $f(2) = 2$, or $f(1) = 2$ and $f(2) = 1$. Similarly, we must have $f(5) = 5$ and $f(6) = 6$, or $f(5) = 6$ and $f(6) = 5$. Furthermore, 3 precedes 4 and they both must succeed 1 and 2 and they both must precede 5 and 6. Thus we must have $f(3) = 3$ and $f(4) = 4$. In other words, $n = 4$. The four similarity mappings are listed in Fig. 7-18(b).

(b) S with the inverse order is pictured in Fig. 7-18(c), which may be obtained by inverting the original diagram which reverses the direction of the arrows. Clearly the diagrams are order-isomorphic. One such order-isomorphism between the sets follows:

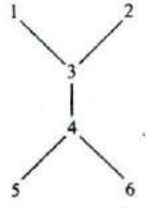
$$f(1) = 5, \quad f(2) = 6, \quad f(3) = 4, \quad f(4) = 3, \quad f(5) = 1, \quad f(6) = 2$$



(a)

$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$
1	2	3	4	5	6
2	1	3	4	5	6
1	2	3	4	6	5
1	2	3	4	5	6

(b)



(c)

Fig. 7-18

7.30. Consider $\mathbf{P} = \{1, 2, 3, \ldots\}$ and $\mathbf{A} = \{a, b, c, \ldots, x, y\}$ with the usual orders, and suppose $S = \mathbf{P} \cup \mathbf{A}$ and $T = \mathbf{A} \cup \mathbf{P}$ are each given the concatenation order

$$S = \{1, 2, 3, \ldots; a, b, \ldots, z\} \quad \text{and} \quad T = \{a, b, \ldots, z; 1, 2, 3, \ldots\}$$

Show that S and T are not order-isomorphic.

There are two elements, 1 and a, which have no predecessors in S, but there is only one element, a, which has no predecessor in T. Any order-isomorphism between sets must preserve the number of such elements. Thus S is not order-isomorphic to T.

7.31. Let A be an ordered set and, for each $a \in A$, let $p(a)$ denote the set of predecessors of a:

$$p(a) = \{x : x \leq a\}$$

(called the *predecessor set* of a). Let $p(A)$ denote the collection of all predecessor sets of the elements in A ordered by set inclusion. Show that A and $p(A)$ are isomorphic by showing that the map $f: A \to p(A)$, defined by $f(a) = p(a)$, is a similarity mapping of A onto $p(A)$.

First we show that f preserves the order relation of A. Suppose $a \leq b$. Let $x \in p(a)$. Then $x \leq a$, and hence $x \leq b$; so $x \in p(b)$. Thus $p(a) \subseteq p(b)$. Suppose $a \| b$ (noncomparable). Then $a \in p(a)$ but $a \notin p(b)$; hence $p(a) \not\subseteq p(b)$. Similarly, $b \in p(b)$ but $b \notin p(a)$; hence $p(b) \not\subseteq p(a)$. Therefore, $p(a) \| p(b)$. Thus f preserves order.

We now need only show that f is a one-to-one and onto. First we show that f is an onto function. Suppose $y \in p(A)$. Then $y = p(a)$ for some $a \in A$. Thus $f(a) = p(a) = y$ so f is a function from A onto $p(A)$.

Next we show f is one-to-one. Suppose $a \neq b$. Then $a < b$, $b > a$ or $a \| b$. In the first and third cases, $b \in p(b)$ but $b \notin p(a)$, and in the second case $a \in p(a)$ but $a \notin p(b)$. Accordingly, in all three cases, we have $p(a) \neq p(b)$. Therefore f is one-to-one.

Consequently, f is a similarity mapping of A onto $p(A)$ and so $A \simeq p(A)$.

7.32. Consider the ordered set $A = \{a, b, c, d, e\}$ in Fig. 7-19(*a*). Find the Hasse diagram of the collection $p(A)$ of predecessor sets of the elements of A ordered by set inclusion.

The elements of $p(A)$ follow:

$$p(a) = \{a, c, d, e\}, \quad p(b) = \{b, c, d, e\}, \quad p(c) = \{c, d, e\}, \quad p(d) = \{d\}, \quad p(e) = \{e\}$$

Figure 7-19(*b*) gives the diagram of $p(A)$ ordered by set inclusion. Observe that the two diagrams in Fig. 7-19 are identical except for the labeling of the vertices.

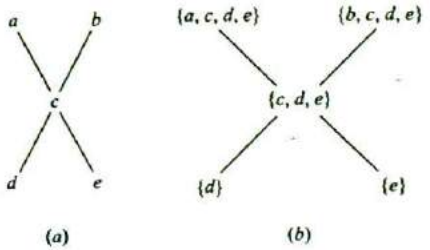


Fig. 7-19

LATTICES

7.33. Write the dual of each statement:

(*a*) $(a \wedge b) \vee c = (b \vee c) \wedge (c \vee a)$; (*b*) $(a \wedge b) \vee a = a \wedge (b \vee a)$

Replace $\vee$ by $\wedge$ and $\wedge$ by $\vee$ in each statement to obtain the dual statement:

(*a*) $(a \vee b) \wedge c = (b \wedge c) \vee (c \wedge a)$

(*b*) $(a \vee b) \wedge a = a \vee (b \wedge a)$

7.34. Give an example of an infinite lattice L with finite length.

Let $L = \{0, 1, a_1, a_2, a_3, \ldots\}$ and let L be ordered as in Fig. 7-20; that is, for each $n \in \mathbf{P}$ we have

$$0 < a_n < 1$$

Then L has finite length since L has no infinite linearly ordered subset.

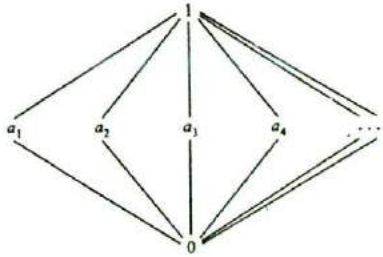


Fig. 7-20

7.35. Prove Theorem 7.8: Let L be a lattice. Then: (i) $a \wedge b = a$ if and only if $a \vee b = b$. (ii) The relation $a \leq b$ (defined by $a \wedge b = a$ or $a \vee b = b$) is a partial order on L.

(*a*) Suppose $a \wedge b = a$. Using the absorption law in the first step we have:

$$b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$$

Now suppose $a \vee b = b$. Again using the absorption law in the first step we have:

$$a = a \wedge (a \vee b) = a \wedge b$$

Thus $a \wedge b = a$ if and only if $a \vee b = b$.

(*b*) For any a in L, we have $a \wedge a = a$ by idempotency. Hence $a \leq a$, and so $\leq$ is reflexive.

Suppose $a \leq b$ and $b \leq a$. Then $a \wedge b = a$ and $b \wedge a = b$. Therefore, $a = a \wedge b = b \wedge a = b$, and so $\leq$ is antisymmetric.

Lastly, suppose $a \leq b$ and $b \leq c$. Then $a \wedge b = a$ and $b \wedge c = b$. Thus

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$$

Therefore $a \leq c$, and so $\leq$ is transitive. Accordingly, $\leq$ is a partial order on L.

7.36. Which of the partially ordered sets in Fig. 7-21 are lattices?

A partially ordered set is a lattice if and only if $\sup(x, y)$ and $\inf(x, y)$ exist for each pair x, y in the set. Only (*c*) is not a lattice since $\{a, b\}$ has three upper bounds, c, d, and I, and no one of them precedes the other two, i.e., $\sup(a, b)$ does not exist.

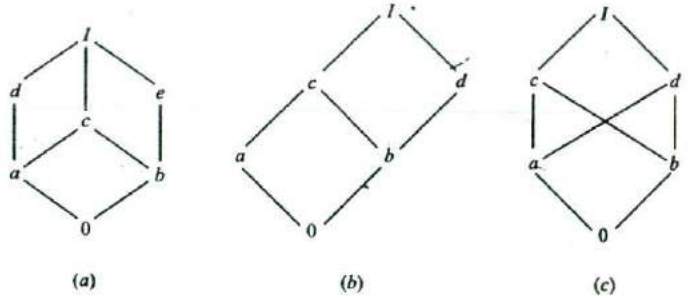


Fig. 7-21

7.37. Consider the lattice L in Fig. 7-21(*a*).

(*a*) Which nonzero elements are join irreducible?

(*b*) Which elements are atoms?

(*c*) Which of the following are sublattices of L:

$$L_1 = \{0, a, b, I\} \qquad L_3 = \{a, c, d, I\}$$
$$L_2 = \{0, a, e, I\} \qquad L_4 = \{0, c, d, I\}$$

(*d*) Is L distributive?

(*e*) Find complements, if they exist, for the elements a, b, and c.

(*f*) Is L a complemented lattice?

(*a*) Those nonzero elements with a unique immediate predecessor are join irreducible. Hence a, b, d, and e are join irreducible.

(*b*) Those elements which immediately succeed 0 are atoms, hence a and b are the atoms.

(c) A subset L' is a sublattice if it is closed under $\wedge$ and $\vee$. L_1 is not a sublattice since $a \vee b = c$, which does not belong to L_1. The set L_4 is not a sublattice since $c \wedge d = a$ does not belong to L_4. The other two sets, L_2 and L_3, are sublattices.

(d) L is not distributive since $M = \{0, a, d, e, I\}$ is a sublattice which is isomorphic to the nondistributive lattice in Fig. 7-7(a).

(e) We have $a \wedge e = 0$ and $a \vee e = I$, so a and e are complements. Also b and d are complements. However, c has no complement.

(f) L is not a complemented lattice since c has no complement.

7.38. Consider the lattice M in Fig. 7-21(b).

(a) Find the nonzero join-irreducible elements and atoms of M.

(b) Is M distributive?

(c) Is M complemented?

(a) The nonzero elements with a unique predecessor are a, b, and d, and of these three only a and b are atoms since their unique predecessor is 0.

(b) M is distributive since M does not have a sublattice which is isomorphic to one of the lattices in Fig. 7-7.

(c) M is not complemented since b has no complement. Note a is the only solution to $b \wedge x = 0$ but $b \vee a = c \neq I$.

7.39. Prove Theorem 7.12: Let L be a finite distributive lattice. Then every a in L can be written uniquely (except for order) as the join of irredundant join-irreducible elements.

Since L is infinite we can write a as the join of irredundant join-irreducible elements as discussed in Section 7.11. Thus we need only prove uniqueness. Suppose

$$a = b_1 \vee b_2 \vee \cdots \vee b_r = c_1 \vee c_2 \vee \cdots \vee c_s$$

where the b's are irredundant and join irreducible and the c's are irredundant and irreducible. For any given i we have

$$b_i \leq (b_1 \vee b_2 \vee \cdots \vee b_r) = (c_1 \vee c_2 \vee \cdots \vee c_s)$$

Hence

$$b_i = b_i \wedge (c_1 \vee c_2 \vee \cdots \vee c_s) = (b_i \wedge c_1) \vee (b_i \wedge c_2) \vee \cdots \vee (b_i \wedge c_s)$$

Since b_i is join irreducible, there exists a j such that $b_i = b_i \wedge c_j$, and so $b_i \leq c_j$. By a similar argument, for c_j there exists a b_k such that $c_j \leq b_k$. Therefore

$$b_i \leq c_j \leq b_k$$

which gives $b_i = c_j = b_k$ since the b's are irredundant. Accordingly, the b's and c's may be paired off. Thus the representation for a is unique except for order.

7.40. Prove Theorem 7.14: Let L be a complemented lattice with unique complements. Then the join-irreducible elements of L, other than 0, are its atoms.

Suppose a is join irreducible and is not an atom. Then a has a unique immediate predecessor $b \neq 0$. Let b' be the complement of b. Since $b \neq 0$ we have $b' \neq I$. If a precedes b', then $b \leq a \leq b'$, and so $b \wedge b' = b'$, which is impossible since $b \wedge b' = I$. Thus a does not precede b', and so $a \wedge b'$ must strictly precede a. Since b is the unique immediate predecessor of a, we also have that $a \wedge b'$ precedes b as in Fig. 7-22. But $a \wedge b'$ precedes b'. Hence

$$a \wedge b' \leq \inf(b, b') = b \wedge b' = 0$$

Thus $a \wedge b' = 0$. Since $a \vee b = a$, we also have that

$$a \vee b' = (a \vee b) \vee b' = a \vee (b \vee b') = a \vee I = I$$

Therefore b' is a complement of a. Since complements are unique, $a = b$. This contradicts the assumption that b is an immediate predecessor of a. Thus the only join-irreducible elements of L are its atoms.

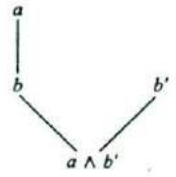


Fig. 7-22

Supplementary Problems

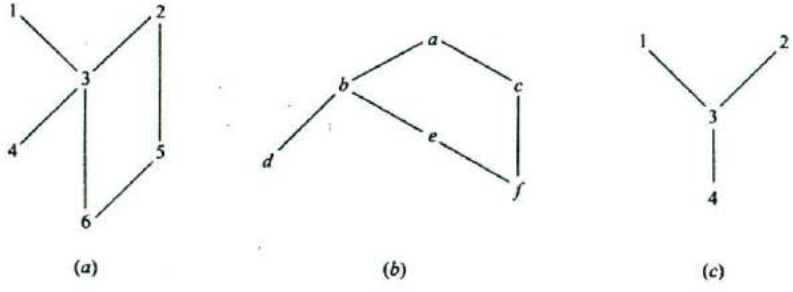
ORDERED SETS AND SUBSETS

7.41. Let $A = \{1, 2, 3, 4, 5, 6\}$ be ordered as in Fig. 7-23(a).

(a) Find all minimal and maximal elements of A.

(b) Does A have a first or last element?

(c) Find all linearly ordered subsets of A, each of which contains at least three elements.



(a) (b) (c)

Fig. 7-23

7.42. Let $B = \{a, b, c, d, e, f\}$ be ordered as in Fig. 7-23(b).

(a) Find all minimal and maximal elements of B.

(b) Does B have a first or last element?

(c) List two and find the number of consistent enumerations of B into the set $\{1, 2, 3, 4, 5, 6\}$.

7.43. Let $C = \{1, 2, 3, 4\}$ be ordered as in Fig. 7-23(c). Let $L(C)$ denote the collection of all nonempty chains in C ordered by set inclusion. Draw a diagram of $L(C)$.

7.44. Draw the diagrams of the partitions of m (see Example 7.4) where: (a) $m = 4$; (b) $m = 6$.

7.45. Let $\mathbf{D}_m$ denote the positive divisors of m ordered by divisibility. Draw the Hasse diagrams of:

(a) $\mathbf{D}_{12}$; (b) $\mathbf{D}_{15}$; (c) $\mathbf{D}_{16}$; (d) $\mathbf{D}_{17}$.

7.46. Let $S = \{a, b, c, d, e, f\}$ be an ordered set. Suppose, under the relation $<<$ (immediately precedes), there are exactly six pairs of elements as follows:

$$f << a, \quad f << d, \quad e << b, \quad c << f, \quad e << c, \quad b << f$$

(*a*) Find all minimal and maximal elements of S.

(*b*) Does S have any first or last element?

(*c*) Find all pairs of elements, if any, which are noncomparable.

7.47. State whether each of the following is true or false and, if it is false, give a counterexample.

(*a*) If an ordered set S has only one maximal element a, then a is a last element.

(*b*) If a finite ordered set S has only one maximal element a, then a is a last element.

(*c*) If a linearly ordered set S has only one maximal element a, then a is a last element.

7.48. Let $S = \{a, b, c, d, e\}$ be ordered as in Fig. 7-24(*a*).

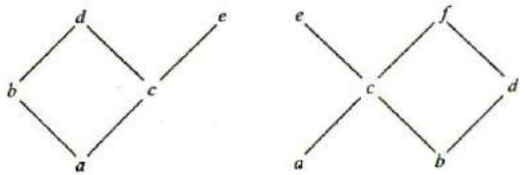
(*a*) Find all minimal and maximal elements of S.

(*b*) Does S have any first or last element?

(*c*) Find all subsets of S in which c is a minimal element.

(*d*) Find all subsets of S in which c is a first element.

(*e*) List all linearly ordered subsets with three or more elements.



(*a*) (*b*)

Fig. 7-24

7.49. Let $S = \{a, b, c, d, e, f\}$ be ordered as in Fig. 7-24(*b*)

(*a*) Find all minimal and maximal elements of S.

(*b*) Does S have any first or last element?

(*c*) List all chains (linearly ordered subsets) with three or more elements.

7.50. Let $S = \{a, b, c, d, e, f, g\}$ be ordered as in Fig. 7-15. Find the number n of chains in S with:

(*a*) four elements; (*b*) five elements.

7.51. Let $S = \{1, 2, \ldots, 7, 8\}$ be ordered as in Fig. 7-16. Find the number n of chains in S with:

(*a*) five elements; (*b*) six elements.

7.52. Give an example of an ordered set with one minimal element but no first element.

CONSISTENT ENUMERATIONS

7.53. Let $S = \{a, b, c, d, e\}$ be ordered as in Fig. 7.24(*a*). List all consistent enumerations of S into $\{1, 2, 3, 4, 5\}$

7.54. Let $S = \{a, b, c, d, e, f\}$ be ordered as in Fig. 7-24(*b*). Find the number n of consistent enumerations of into $\{1, 2, 3, 4, 5, 6\}$.

7.55. Suppose the following are three consistent enumerations of an ordered set $A = \{a, b, c, d\}$:

$$[(a,1),(b,2),(c,3),(d,4)], \qquad [(a,1),(b,3),(c,2),(d,4)], \qquad [(a,1),(b,4),(c,2),(d,3)]$$

Assuming the Hasse diagram D of A is connected (any two points are connected by a path), draw D.

SET CONSTRUCTIONS AND ORDER

7.56. Let $M = \{2, 3, 4, \ldots\}$ and let $M^2 = M \times M$ be ordered as follows:

$$(a, b) \leq (c, d) \qquad \text{if } a|c \text{ and } b \leq d$$

Find all minimal and maximal elements of $M \times M$.

7.57. Consider the English alphabet $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ with the usual (alphabetical) order. Recall that the Kleene closure $\mathbf{A}^*$ consists of all words in $\mathbf{A}$. Let L consist of the following elements in $\mathbf{A}^*$:

gone, or, arm, go, an, about, gate, one, at, occur

(*a*) Sort L according to the short-lex order, i.e., first by length and then alphabetically.

(*b*) Sort L alphabetically.

7.58. Consider the ordered sets A and B appearing in Fig. 7-23(*a*) and (*b*), respectively. Suppose $S = A \times B$ is given the product order, i.e.,

$$(a, b) \leq (a', b') \qquad \text{if } a \leq a' \text{ and } b \leq b'$$

Insert the correct symbol, $<$, $>$, or $\|$, between each pair of elements of S:

(*a*) $(4, b)$ ____ $(2, e)$ (*c*) $(5, d)$ ____ $(1, a)$

(*b*) $(3, a)$ ____ $(6, f)$ (*d*) $(6, e)$ ____ $(2, b)$

7.59. Suppose $\mathbf{P} = \{1, 2, 3, \ldots\}$ and $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ are given the usual orders, and $S = \mathbf{P} \times \mathbf{A}$ is ordered lexicographically. Sort the following elements of S:

$$(2, z), (1, c), (2, c), (1, y), (4, b), (4, z), (3, b), (2, a)$$

7.60. Consider the set $\mathbf{P}$ of positive integers, the English alphabet $\mathbf{A}$, and the set B of negative integers with the usual orders:

$$\mathbf{P} = \{1, 2, 3, \ldots\}, \qquad \mathbf{A} = \{a, b, c, \ldots, y, z\}, \qquad B = \{\ldots, -3, -2, -1\}$$

Suppose $S = \mathbf{P} \cup \mathbf{A} \cup B$, $T = \mathbf{P} \cup B \cup \mathbf{A}$, $U = B \cup \mathbf{A} \cup \mathbf{P}$, $V = B \cup \mathbf{P} \cup \mathbf{A}$ are each given the concatenation order. (Here the sets $\mathbf{P}, \mathbf{A}, B$ in S, T, U, V are ordered as shown in the union.)

(*a*) Which of the sets S, T, U, V has a minimal element?

(*b*) Which of the sets S, T, U, V has a maximal element?

(*c*) Which element or elements in the sets S, T, U, V have no immediate predecessor?

(*d*) Which element or elements in the sets S, T, U, V have no immediate successor?

UPPER AND LOWER BOUNDS, SUPREMUM AND INFIMUM

7.61. Let $S = \{a, b, c, d, e, f, g\}$ be ordered as in Fig. 7-15. Consider the subset $A = \{a, c, d\}$ of S.

(*a*) Find the set of upper bounds of A. (*c*) Does $\sup(A)$ exist?

(*b*) Find the set of lower bounds of A. (*d*) Does $\inf(A)$ exist?

7.62. Repeat Problem 7.61 for subset $B = \{b, c, e\}$ of S.

7.63. Let $S = \{1,2,\ldots,7,8\}$ be ordered as in Fig. 7-16. Consider the subset $A = \{3,6,7\}$ of S.

(*a*) Find the set of upper bounds of A. (*c*) Does $\sup(A)$ exist?

(*b*) Find the set of lower bounds of A. (*d*) Does $\inf(A)$ exist?

7.64. Repeat Problem 7.63 for the subset $B = \{1,2,4,7\}$ of S.

7.65. Consider the set $\mathbf{Q}$ of rational numbers with the usual order $\leq$. Let $A = \{x \in \mathbf{Q} : 5 < x^3 < 27\}$.

(*a*) Is A bounded above or below? (*b*) Do $\sup(A)$ and $\inf(A)$ exist?

7.66. Consider the set $\mathbf{R}$ of real numbers with the usual order $\leq$. Let $B = \{x \in \mathbf{R} : x \in \mathbf{Q} \text{ and } 5 < x^3 < 27\}$.

(*a*) Is B bounded above or below? (*b*) Do $\sup(B)$ and $\inf(B)$ exist?

ORDER-ISOMORPHIC SETS, SIMILARITY MAPPINGS

7.67. Let S be the ordered set in Fig. 7-24(*a*). Suppose $A = \{1,2,3,4,5\}$ is order-isomorphic to S and the following is a similarity mapping from S onto A:

$$f = \{(a,1),(b,4),(c,5),(d,2),(e,3)\}$$

Draw the Hasse diagram of A.

7.68. Find the number of nonisomorphic ordered sets with three elements a, b, c, and draw their diagrams.

7.69. Find the number of connected nonisomorphic ordered sets with four elements a, b, c, d, and draw their diagrams.

7.70. Find the number of similarity mappings $f: S \to S$ if S is the ordered set in:

(*a*) Fig. 7-23(*a*); (*b*) Fig. 7-23(*b*); (*c*) Fig. 7-23(*c*).

7.71. Suppose $\mathbf{P} = \{1,2,3,\ldots\}$ and $\mathbf{A} = \{a,b,c,\ldots,z\}$ are given the usual orders, and each of $S = \mathbf{P} \cup \mathbf{A}$ and $T = \mathbf{A} \cup \mathbf{P}$ is given the concatenation order. Which of the sets $\mathbf{P}$, $\mathbf{A}$, S, T are order-isomorphic?

7.72. Which of the sets S, T, U, V in Problem 7.60 are order-isomorphic?

7.73. Determine whether or not $\zeta = \zeta^*$ where ζ is the order type of each of the following sets (with the usual order):

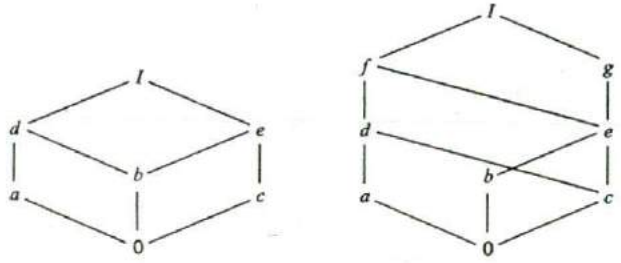
(*a*) $\mathbf{R}$; (*b*) $A = \{\ldots,-3,-2,-1\}$; (*c*) $B = \{\ldots,-4,-2,0,2,4,\ldots\}$.

7.74. Determine which of the sets in Problem 7.73 have the same order type as: (*a*) $\mathbf{P}$; (*b*) $\mathbf{Z}$. (*c*) $\mathbf{Q}$.

7.75. Let C be the ordered set in Fig. 7-23(*c*). (*a*) Draw the Hasse diagram of the collection $p(C)$ of predecessor sets ordered by set inclusion. (*b*) Is C order isomorphic to $p(C)$?

LATTICES

7.76. Consider the lattice L in Fig. 7-25(a). (a) Find all sublattices with five elements. (b) Find all join-irreducible elements, and atoms. (c) Find complements of a and b, if they exist. (d) Is L distributive? Complemented?



(a) (b)

Fig. 7-25

7.77. Consider the lattice M in Fig. 7-25(b). (a) Find join-irreducible elements. (b) Find the atoms. (c) Find complements of a and b, if they exist. (d) Express each x in M as the join of irredundant join-irreducible elements. (e) Is M distributive? Complemented?

7.78. Consider the bounded lattice L in Fig. 7-26(a).

(a) Find the complements, if they exist, of e and f.

(b) Express I in an irredundant join-irreducible decomposition in as many ways as possible.

(c) Is L distributive?

(d) Describe the isomorphisms of L with itself.

7.79. Consider the bounded lattice L in Fig. 7-26(b).

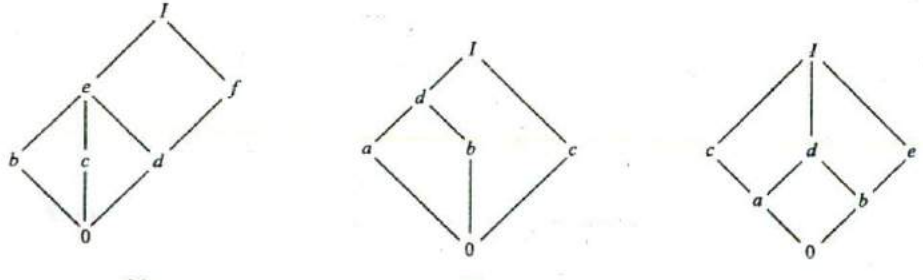
(a) Find the complements, if they exist, of a and c.

(b) Express I in an irredundant join-irreducible decomposition in as many ways as possible.

(c) Is L distributive?

(d) Describe the isomorphisms of L with itself.

7.80. Redo Problem 7.79 for the bounded lattice L in Fig. 7-26(c).



(a) (b) (c)

Fig. 7-26

7.81. Let $\mathbf{D}_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$, the divisors of 60, be ordered by divisibility.

(*a*) Draw the Hasse diagram of $\mathbf{D}_{60}$.

(*b*) Which elements are join-irreducible? Atoms?

(*c*) Find the complements of 2 and 10, if they exist.

(*d*) Express each number x as the join of a minimum number of irredundant join-irreducible elements.

7.82. Consider the lattice **P** of positive integers ordered by divisibility. (*a*) Which elements are join-irreducible? (*b*) Which elements are atoms?

7.83. Show that the following "weak" distributive laws hold for any lattice:

(*a*) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \wedge c)$

(*b*) $a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)$

7.84. Let $S = \{1, 2, 3, 4\}$. Three partitions of S follow:

$$P_1 = [12, 3, 4], \qquad P_2 = [12, 34], \qquad P_3 = [13, 2, 4]$$

(Here [12, 3, 4] is short for $[\{1, 2\}, \{3\}, \{4, \}]$.)

(*a*) Find the other nine partitions of S.

(*b*) Let L be the collection of the twelve partitions of S ordered by *refinement*, that is, $P_i \leq P_j$ if each cell of P_i is a subset of a cell of P_j. For example, $P_1 \leq P_2$, but P_2 and P_3 are noncomparable. Show that L is a bounded lattice and draw its Hasse diagram.

7.85. An element a in a lattice L is said to be *meet-irreducible* if $a = x \wedge y$ implies $a = x$ or $a = y$. Find all meet-irreducible elements in: (*a*) Fig. 7-25(*a*); (*b*) Fig. 7-25(*b*); (*c*) $\mathbf{D}_{60}$ (see Problem 7.81).

7.86. A lattice M is said to be *modular* if whenever $a \leq c$ we have the law

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

(*a*) Prove that every distributive lattice is modular.

(*b*) Verify that the nondistributive lattice in Fig. 7-7(*b*) is modular; hence the converse of (*a*) is not true.

(*c*) Show that the nondistributive lattice in Fig. 7-7(*a*) is nonmodular. [In fact, one can prove that every nonmodular lattice contains a sublattice isomorphic to Fig. 7-7(*a*).]

Answers to Supplementary Problems

7.41. (*a*) Minimal: 4 and 6; Maximal: 1 and 2. (*b*) First: none; Last: none. (*c*) $\{1, 3, 4\}$, $\{1, 3, 6\}$, $\{2, 3, 4\}$, $\{2, 3, 6\}$, $\{2, 5, 6\}$.

7.42. (*a*) Minimal: d and f; Maximal: a. (*b*) First: none; Last: a. (*c*) There are eleven: *dfebca*, *dfecba*, *dfceba*, *fdebca*, *fdecba*, *fdceba*, *fedbca*, *fedcba*, *fcdeba*, *fecdba*, *fcedba*.

7.43. See Fig. 7-27.

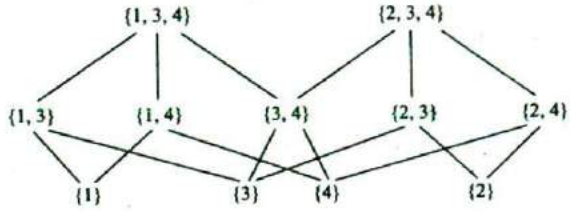


Fig. 7-27

7.44. See Fig. 7-28.

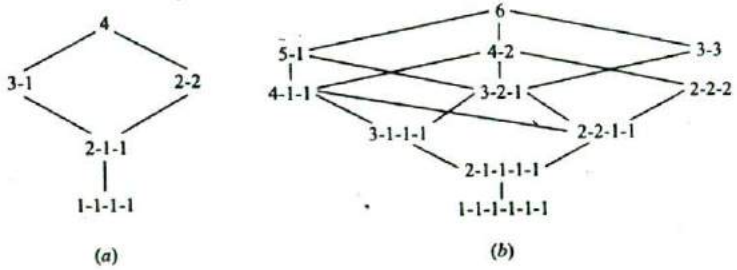


Fig. 7-28

7.45. See Fig. 7-29.

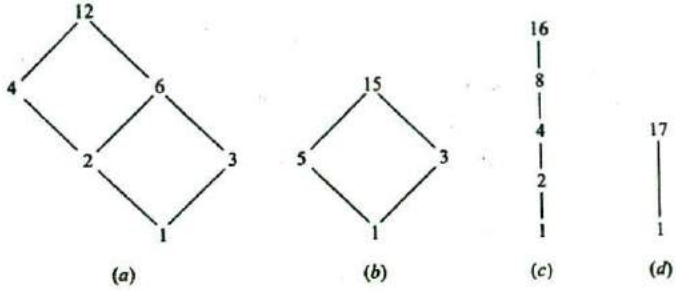


Fig. 7-29

7.46. Hint: Draw diagram of S. (*a*) Minimal: e; Maximal: a, d. (*b*) First: e; Last: none. (*c*) $\{a, d\}$, $\{b, c\}$.

7.47. (*a*) False. Example: $\mathbf{P} \cup \{a\}$ where $1 << a$, and $\mathbf{P}$ ordered by $\leq$. (*b*) True. (*c*) True.

7.48. (*a*) Minimal: a; Maximal: d and e. (*b*) First: a; Last: none. (*c*) Any subset which contains c and omits a; that is, c, cb, cd, ce, cbd, cbe, cde, $cbde$. (*d*) c, cd, ce, cde. (*e*) abd, acd, ace.

7.49. (*a*) Minimal: a and b; Maximal: e and f. (*b*) First: none; Last: none. (*c*) ace, acf, bce, bcf, bdf.

7.50. (*a*) Four; (*b*) none

7.51. (*a*) Six; (*b*) none

7.52. $S = \{a\} \cup A$ where $A = \{\ldots, -3, -2, -1, 0\}$ has the usual order and where $a << 0$.

7.53. *abcde, abced, acbde, acbed, acebd*

7.54. Eleven

7.55. $a << b$, $a << c$, $c << d$

7.56. Minimal: $(p, 2)$ where p is a prime. Maximal: none.

7.57. (*a*) an, at, go, or, arm, one, gate, gone, about, occur
(*b*) an, about, arm, at, gate, go, gone, occur, one, or

7.58. (*a*) $\|$; (*b*) $>$; (*c*) $\|$; (*d*) $<$

7.59. $1c, 1y, 2a, 2c, 2z, 3b, 4b, 4z$

7.60. (*a*) S and T; (*b*) T and V; (*c*) $1, a \in S$, $1 \in T$, $a \in V$; (*d*) $-1, z \in S$, $z \in T$, $z \in V$

7.61. (*a*) e, f, g; (*b*) a; (*c*) $\sup(A) = e$; (*d*) $\inf(A) = a$

7.62. (*a*) e, f, g; (*b*) none; (*c*) $\sup(B) = e$; (*d*) none

7.63. (*a*) 1, 2, 3; (*b*) 8; (*c*) $\sup(A) = 3$; (*d*) $\inf(A) = 8$

7.64. (*a*) None; (*b*) 8; (*c*) none; (*d*) $\inf(B) = 8$

7.65. (*a*) Both; (*b*) $\sup(A) = 3$, $\inf(A)$ does not exist.

7.66. (*a*) Both; (*b*) $\sup(A) = 3$, $\inf(A) = \sqrt[3]{5}$.

7.67. See Fig. 7-30.

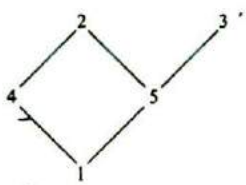


Fig. 7-30

7.68. Four: (1) a, b, c; (2) $a, b << c$; (3) $a << b$, $a << c$; (4) $a << b << c$.

7.69. Four: See Fig. 7-31.

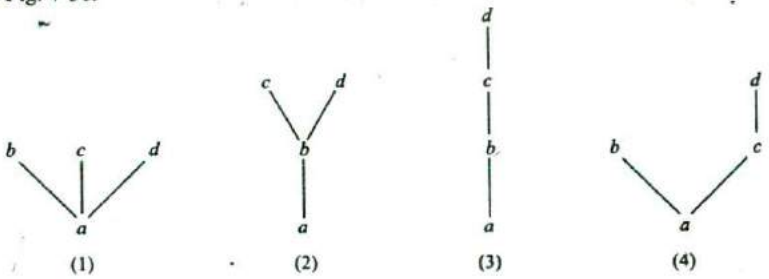


Fig. 7-31

7.70. (*a*) One: identity mapping; (*b*) one; (*c*) two

7.71. **P** and T

7.72. None

7.73. (*a*) Yes; (*b*) no; (*c*) yes

7.74. (*a*) None; (*b*) B; (*c*) none

7.75. (*a*) See Fig. 7-32; (*b*) yes (always)

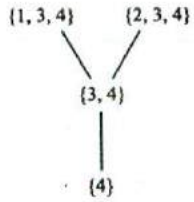


Fig. 7-32

7.76. (*a*) Six: $0abdI, 0acdI, 0adeI, 0bceI, 0aceI, 0cdeI$
(*b*) (i) $a, b, e, 0$; (iii) a, b, c
(*c*) c and e are complements of a; b has no complement.
(*d*) No; no

7.77. (*a*) $a, b, c, g, 0$; (*b*) a, b, c; (*c*) g is the complement of a; b has no complement.
(*d*) $I = a \vee g, f = a \vee b = a \vee c, e = b \vee c, d = a \vee c$; other elements are join irreducible. (*e*) No; no

7.78. (*a*) e has none; f has b and c.
(*b*) $I = c \vee d \vee f = b \vee c \vee f = b \vee d \vee f$
(*c*) No, since decompositions are not unique.
(*d*) Two: 0, d, e, f, I must be mapped into themselves. Then $F = 1_L$, identity map on L, or $F = \{(b, c), (c, b)\}$.

7.79. (*a*) a has c; c has a and b. (*b*) $I = a \vee c = b \vee c$.
(*c*) No. (*d*) Two: 0, c, d, I must be mapped into themselves. Then $f = 1_L$ or $f = \{(a, b), (b, a)\}$.

7.80. (*a*) a has e, c has b and e. (*b*) $I = a \vee e = b \vee c = c \vee e$. (*c*) No.
(*d*) Two: 0, d, I are mapped into themselves. Then $f = 1_L$ or $f = \{(a,b),(b,a),(c,d),(d,c)\}$.

7.81. (*a*) See Fig. 7-33. (*b*) 1, 2, 3, 4, 5; the atoms are 2, 3, and 5. (*c*) 2 has none, 10 has 3.

(*d*) $60 = 4 \vee 3 \vee 5 \quad 30 = 2 \vee 3 \vee 5 \quad 20 = 4 \vee 5$
$15 = 3 \vee 5 \quad 12 = 3 \vee 4 \quad 10 = 2 \vee 5 \quad 6 = 2 \vee 3$

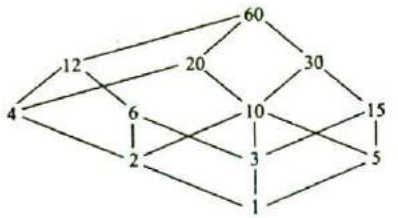


Fig. 7-33

7.82. (*a*) Powers of primes and 1; (*b*) primes

7.84. (*a*) [1, 2, 3, 4], [14, 2, 3], [13, 24], [14, 23], [123, 4], [124, 3], [134, 2], [234, 1], [1234]
(*b*) See Fig. 7-34.

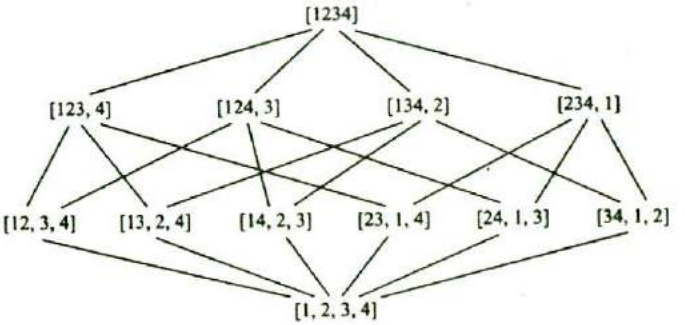


Fig. 7-34

7.85. Geometrically, an element $a \neq I$ is meet-irreducible if and only if a has only one immediate successor:
(*a*) a, c, d, e, I; (*b*) a, b, d, f, g, I; (*c*) 4, 6, 10, 12, 15, 60.

7.86. (*a*) If $a \leq c$ then $a \vee c = c$. Hence

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$$

(*c*) Here $a \leq c$. But $a \vee (b \wedge c) = a \vee 0 = a$ and $(a \vee b) \wedge c = I \wedge c = c$; hence

$$a \vee (b \wedge c) \neq (a \vee b) \wedge c$$

Chapter 8

Ordinal Numbers

8.1 INTRODUCTION

Numbers are usually used for two different things. One is to measure quantity, such as the number of students in a class, and the other is to indicate order, such as the first student, the second student, and so on. Cardinal numbers, covered in Chapter 6, essentially measure quantity, whereas ordinal numbers, covered in this chapter, indicate order. First, however, it is necessary to discuss a special kind of an ordered set, called a well-ordered set.

8.2 WELL-ORDERED SETS

Not every ordered set, even if it is linearly ordered, need have a first element. For example, $\mathbf{Z}$ is linearly ordered but it does not have a first element. On the other hand, one of the fundamental properties of the set

$$\mathbf{P} = \{1, 2, 3, \ldots\}$$

of counting numbers (positive integers) is that $\mathbf{P}$ and every subset of $\mathbf{P}$ has a first element. Such an ordered set is said to be well-ordered. Namely:

Definition 8.1: Let A be an ordered set. Then A is said to be *well-ordered* if every subset of A contains a first element.

Note that any well-ordered set A is linearly ordered. For if $a, b \in A$, then the subset $\{a, b\}$ of A has a first element which, therefore, must precede the other; hence any two elements of A are comparable.

The following theorem follows directly from the above definition.

Theorem 8.1: Let A be a well-ordered set. Then:

(i) Every subset of A is well-ordered.

(ii) If B is similar to A, then B is well-ordered.

EXAMPLE 8.1 Consider the following two subsets of the well-ordered set $\mathbf{P}$:

$$A_1 = \{1, 3, 5, \ldots\} \quad \text{and} \quad A_2 = \{2, 4, 6, \ldots\}$$

Then A_1 and A_2 are also well-ordered. Suppose the union

$$S = A_1 \cup A_2 = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

is ordered from left to right, as shown. Then S is also well-ordered. This shows that a set, such as $\mathbf{P} = A_1 \cup A_2$, can be well-ordered in more than one way.

Suppose $\{A_i : i \in I\}$ is a linearly ordered collection of disjoint linearly ordered sets, that is, I is linearly ordered and each A_i is linearly ordered. Then the union $S = \bigcup_i A_i$ will be linearly ordered as follows:

$$a < b \quad \text{if} \begin{cases} a \in A_i,\ b \in A_j,\ i < j \\ a, b \in A_i,\ a < b \text{ in } A_i \end{cases}$$

This ordering will be called the *usual ordering* on the union S. (It is also called the concatenation or sum ordering on S.) The ordering is somewhat analogous to a lexicographical ordering in the sense that the index ordering has the first priority. This ordering is sometimes pictured by listing the elements of A_i before the elements of A_j when $i < j$. Example 8.1 is an instance of such an ordering and its picture.

The following theorem applies.

Theorem 8.2: Suppose $\{A_i : i \in I\}$ is a well-ordered family of disjoint well-ordered sets, that is, I is well-ordered and each A_i is well-ordered. Then the union $S = \bigcup_i A_i$, with the usual ordering, is well-ordered.

EXAMPLE 8.2 Let $V = \{a_1, a_2, \ldots, a_n\}$ be any finite linearly ordered set. Then V may be written in the form

$$V = \{a_{i_1}, a_{i_2}, \ldots, a_{i_n}\}$$

where the elements are ordered as shown. Notice that V is well-ordered. Furthermore, notice that any other linearly ordered set W with n elements, say

$$W = \{b_{i_1}, b_{i_2}, \ldots, b_{i_n}\}$$

is similar to V.

We formally state the comment in Example 8.3.

Theorem 8.3: All finite linearly ordered sets with the same number n of elements are well-ordered and are similar to each other.

8.3 TRANSFINITE INDUCTION

The reader is familiar with the principle of mathematical induction. Namely:

Principle of Mathematical Induction: Let S be a subset of the set $\mathbf{P}$ of counting numbers with the following two properties:

(1) $1 \in S$.
(2) If $n \in S$, then $n + 1 \in S$.

Then S is the set of all counting numbers, that is, $S = \mathbf{P}$.

The above principle is one of Peano's axioms for the counting numbers $\mathbf{P}$. The principle can be shown to be a consequence of the fact that $\mathbf{P}$ is well-ordered. In fact, there is a somewhat similar statement which is true for any well-ordered set (proved in Problem 8.1).

Theorem 8.4 (Principle of Transfinite Induction): Let S be a subset of a well-ordered set A with the following two properties:

(1) $a_0 \in S$.
(2) If $s(a) \subseteq S$, then $a \in S$.

Then S is the entire set A, that is, $S = A$.

Here a_0 is the first element of A and $s(a)$, called the *initial segment* of a, is defined to be the set of all elements in A which strictly precedes a.

Initial segments will be discussed below, and Chapter 9 will discuss transfinite induction in much more detail.

8.4 LIMIT ELEMENTS

Let A be an ordered set, and let a, b belong to A. Recall that a is called an *immediate predecessor* of b, and that b is called an *immediate successor* of a, written

$$a << b$$

if $a < b$ but no element in A lies between a and b, that is, there does not exist an element c in A such that $a < c < b$.

EXAMPLE 8.3

(*a*) Let $A = \{a, b, c, d, e\}$ be ordered as in Fig. 8-1. Then c is an immediate predecessor of b and c, and b is an immediate successor of d and e.

(*b*) Consider the set $\mathbf{Q}$ of rational numbers with the usual order. Even though $\mathbf{Q}$ is linearly ordered, no element in $\mathbf{Q}$ has an immediate predecessor or an immediate successor. For if $a, b \in \mathbf{Q}$, say $a < b$, then $(a + b)/2$ belongs to $\mathbf{Q}$ and

$$a < (a + b)/2 < b$$

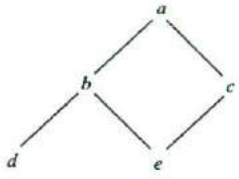


Fig. 8-1

Example 8.3 shows that linearly ordered sets need not have any immediate predecessors or any immediate successors. This is not true in the case of well-ordered sets. That is:

Theorem 8.5: Every element in a well-ordered set A has a unique immediate successor except the last element.

Proof: Let $a \in A$, and let $M(a)$ denote the set of elements of A which strictly succeeds a. If a is not the last element, then $M(a) \neq 0$. Since A is well-ordered, $M(a)$ has a first element, say b. We claim b is an immediate successor of a. Otherwise, there is an element $c \in A$ such that $a < c < b$. Then $c \in M(a)$ and this contradicts the fact that b is the first element of $M(a)$. We claim b is the only immediate successor of a. Otherwise, there is another immediate successor of a, say d. Then $d \in M(a)$ and, since b is a first element of $M(a)$, we have $a < b < d$. This contradicts the assumption that d is an immediate successor of a. Thus the first element b of $M(a)$ is the unique immediate successor of a.

There is no analogous statement to Theorem 8.4 about immediate predecessors, that is, there do exist elements in well-ordered sets, besides the first element, which do not have immediate predecessors. For example, the set

$$S = A_1 \cup A_2 = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

in Example 8.1 is well-ordered, and both 1 and 2 do not have immediate predecessors.

In view of the above comment and example, we introduce the following definition.

Definition 8.2: An element a in a well-ordered set A is called a *limit element* if it does not have an immediate predecessor and if it is not the first element.

According to this definition, the element 2 in the above set $S = A_1 \cup A_2$ is a limit element.

8.5 INITIAL SEGMENTS

Let A be a well-ordered set. The *initial segment* $s(a)$ of an element $a \in A$ consists of all elements in A which strictly precede a. In other words,

$$s(a) = \{x : x \in A, x < a\}$$

Notice that $s(a)$ is a subset of A.

EXAMPLE 8.4 Consider again the well-ordered S in Example 8.1, that is,

$$S = A_1 \cup A_2 = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

Then $s(1) = \varnothing$, $s(5) = \{1, 3\}$, $s(2) = \{1, 3, 5, \ldots\}$, and $s(8) = \{1, 3, 5, \ldots; 2, 4, 6\}$.

One basic property of initial segments is contained in the next theorem (proved in Problem 8.2).

Theorem 8.6: Let $S(A)$ denote the collection of all initial segments of elements in a well-ordered set A, and let $S(A)$ be ordered by set inclusion. Then A is similar (order-isomorphic) to $S(A)$ and, in particular, the function $f: A \to S(A)$ defined by $f(x) = s(x)$ is a similarity mapping between A and $S(A)$.

8.6 SIMILARITY BETWEEN A WELL-ORDERED SET AND ITS SUBSETS

Consider the set $\mathbf{P}$ of counting numbers, and the subset $E = \{2, 4, 6, \ldots\}$ of $\mathbf{P}$. The function $f: \mathbf{P} \to E$ defined by $f(x) = 2x$ is a similarity mapping of $\mathbf{P}$ onto its subset E. Notice that, for every $x \in \mathbf{P}$,

$$x \leq f(x)$$

This property, which is true in general, is the content of the next theorem (proved in Problem 8.3). Namely:

Theorem 8.7: Let A be a well-ordered set, let B be a subset of A, and let the function $f: A \to B$ be a similarity mapping of A onto B. Then, for every $a \in A$,

$$a \leq f(a)$$

The following important properties of well-ordered sets (proved in Problems 8.4 and 8.5) are consequences of the preceding theorem.

Theorem 8.8: Let A and B be similar well-ordered sets. Then there exists only one similarity mapping of A onto B.

Theorem 8.9: A well-ordered set cannot be similar to one of its initial segments.

8.7 COMPARISON OF WELL-ORDERED SETS

The next theorem (proved in Problem 8.12) gives an important relationship between any two well-ordered sets.

Theorem 8.10: Let A and B be well-ordered sets. Then A and B are similar, or one of them is similar to an initial segment of the other.

Suppose A and B are well-ordered sets, and suppose A is similar to an initial segment of B. Then A is said to be *shorter* than B, and B is said to be *longer* than A. With these definitions, Theorem 8.10 can be restated as follows:

Theorem 8.10′: Let A and B be well-ordered sets. Then A is shorter than B, A is similar to B, or A is longer than B.

The preceding theorem can be strengthened as follows:

Theorem 8.11: Let $\mathscr{A}$ be a collection of pairwise nonsimilar well-ordered sets. Then there exists a set A in $\mathscr{A}$ such that A is shorter than every other set in $\mathscr{A}$.

EXAMPLE 8.5

(*a*) Consider two finite well-ordered sets

$$A = \{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad B = \{b_1, b_2, \ldots, b_n\}$$

Suppose $m < n$. Then A is similar to the initial segment $\{b_1, b_2, \ldots, b_m\}$ of B, and hence A would be shorter than B. Similarly, if $m > n$ then A would be longer than B.

(*b*) The set $\mathbf{P} = \{1, 2, 3, \ldots\}$ is shorter than the well-ordered set

$$S = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

since $\mathbf{P}$ is similar to the initial segment $\{1, 3, 5, \ldots\}$ of S.

8.8 ORDINAL NUMBERS

Consider a collection $\mathscr{S}$ of well-ordered sets. Each well-ordered set A in $\mathscr{S}$ is assigned a symbol in such a way that any two well-ordered sets A and B are assigned the same symbol if and only if A and B are similar (order-isomorphic). This symbol is called the *ordinal number* of A. We will write

$$\lambda = \text{ord}(A)$$

to indicate that λ is the ordinal number of A.

Recall (Theorem 7.5) that the relation of similarity (order-isomorphism), denoted by

$$A \simeq B$$

is an equivalence relation in any collection of ordered sets. Thus by the fundamental theorem on equivalence relations, all ordered sets, and in particular all well-ordered sets, are partitioned into disjoint classes of similar sets. One may view an ordinal number as the equivalence class of all similar well-ordered sets.

Recall (Section 7.9) that every linearly ordered set S is assigned an order type. Thus an ordinal number may also be viewed as the order type of a well-ordered set.

Definition 8.3: The ordinal number of each of the well-ordered sets

$$\varnothing, \{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots$$

is denoted by $0, 1, 2, 3, \ldots$ respectively, and is called a *finite* ordinal number. All other ordinals are called *transfinite* numbers.

Definition 8.4: The ordinal number of the set $\mathbf{P}$ of counting numbers is denoted by

$$\omega = \text{ord}(\mathbf{P})$$

Although the symbols $0, 1, 2, 3, \ldots$ are used to denote natural numbers (nonnegative integers), cardinal numbers and, now, ordinal numbers, the context in which the symbols appear determines their particular meaning. Furthermore, since any two finite well-ordered sets with the same number of elements are similar, $0, 1, 2, 3, \ldots$ are the only finite ordinal numbers.

8.9 INEQUALITIES AND ORDINAL NUMBERS

An inequality relation is defined for the ordinal numbers as follows:

Definition 8.5: Let λ and μ be ordinal numbers and let A and B be two well-ordered sets such that $\lambda = \text{ord}(A)$ and $\mu = \text{ord}(B)$. Then

$$\lambda < \mu$$

if A is similar to an initial segment of B.

Accordingly, for $\lambda = \text{ord}(A)$ and $\mu = \text{ord}(B)$, we have the following:

$\lambda < \mu$ if A is shorter than B,
$\lambda = \mu$ if A is similar to B,
$\lambda > \mu$ if A is longer than B,
$\lambda \leq \mu$ if $\lambda < \mu$ or $\lambda = \mu$,
$\lambda \geq \mu$ if $\lambda > \mu$ or $\lambda = \mu$.

EXAMPLE 8.6

(*a*) Consider two finite well-ordered sets A and B, say

$$A = \{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad B = \{b_1, b_2, \ldots, b_n\}$$

Say $m < n$. Then A is similar to the initial segment $\{b_1, b_2, \ldots, b_m\}$ of B. Hence $\text{ord}(A) < \text{ord}(B)$.

In other words, $m < n$ as ordinal numbers if and only if $m < n$ as nonnegative integers. Thus the inequality relation for ordinal numbers is an extension of the inequality relation in the set **N** of natural numbers.

(*b*) Let $\lambda = \text{ord}(S) = \text{ord}(\{1, 3, 5, \ldots; 2, 4, 6, \ldots\})$. Since the set $\mathbf{P} = \{1, 2, 3, \ldots\}$ is similar to the initial segment $\{1, 3, 5, \ldots\}$ of S, we have

$$\omega < \lambda$$

Properties of the Inequality Relation on Ordinal Numbers

Theorem 8.10 tells us that any two well-ordered sets A and B are similar or one of them is similar to an initial segment of the other. Accordingly, the next theorem is a direct consequence of Theorem 8.10 and the above definition.

Theorem 8.12: Any set of ordinal numbers is linearly ordered by the relation $\lambda \leq \mu$

In view of Theorem 8.10, the preceding theorem can be strengthened as follows:

Theorem 8.13: Any set of ordinal numbers is well-ordered by the relation $\lambda \leq \mu$.

Now let λ be any ordinal number and let $s(\lambda)$ denote the set of ordinal numbers less than λ. By the preceding theorem, $s(\lambda)$ is a well-ordered set and, therefore, $\text{ord}(s(\lambda))$ exists.

Question: What is the relationship between λ and $\text{ord}(s(\lambda))$?

The answer is given in the next theorem (proved in Problem 8.16).

Theorem 8.14: Let $s(\lambda)$ be the set of ordinals less than the ordinal λ. Then $\lambda = \text{ord}(s(\lambda))$.

Since the ordinal numbers are themselves well-ordered, every ordinal has an immediate successor. Some nonzero ordinals, for example ω, do not have immediate predecessors; these are called *limit ordinal numbers* or, simply, *limit numbers*.

8.10 ORDINAL ADDITION

An operation of *addition* is defined for ordinal numbers as follows:

Definition 8.6: Let λ and μ be ordinal numbers, and let A and B be disjoint sets such that $\lambda = \text{ord}(A)$ and $\mu = \text{ord}(B)$. Then

$$\lambda + \mu = \text{ord}(\{A; B\})$$

Recall that $\{A; B\}$ is given the usual order where every element of A precedes every element of B.

EXAMPLE 8.7 Recall $\omega = \text{ord}(P) = \text{ord}(\{1, 2, \ldots\})$ and $n = \text{ord}(\{a_1, a_2, \ldots, a_n\})$. Then

$$n + \omega = \text{ord}(\{a_1, a_2, \ldots, a_n; 1, 2, \ldots\}) = \omega$$

But

$$\omega + n = \text{ord}(\{1, 2, \ldots; a_1, a_2, \ldots, a_n\}) > \omega$$

since **P** is similar to $s(a_1)$, the initial segment of a_1.

Example 8.7 tells us that the operation of addition of ordinal numbers is not commutative. However, the following conditions do hold.

Theorem 8.15: (1) Addition of ordinal numbers satisfies the associative law, i.e.,

$$(\lambda + \mu) + \eta = \lambda + (\mu + \eta)$$

(2) The ordinal 0 is an additive identity element, i.e.,

$$0 + \lambda = \lambda + 0 = \lambda$$

EXAMPLE 8.8 (Addition of Finite Ordinals) Here we will denote the finite ordinals by

$$0^*, 1^*, 2^*, \ldots$$

Consider, now, two finite well-ordered disjoint sets

$$A = \{a_1, a_2, \ldots, a_m\} \quad \text{and} \quad B = \{b_1, b_2, \ldots, b_n\}$$

Then $m^* = \text{ord}(A)$ and $n^* = \text{ord}(B)$. Therefore,

$$m^* + n^* = \text{ord}(A) + \text{ord}(B) = \text{ord}(\{A; B\}) = (m + n)^*$$

Thus the operation of addition for finite ordinal numbers corresponds to the operation of addition for the set **N** of natural numbers (nonnegative integers).

Note once again that the set of ordinal numbers is itself a well-ordered set; hence every ordinal has an immediate successor. For the finite ordinals, i.e., the natural numbers, it is easily seen that $n + 1$ is the immediate successor to n. The next theorem (proved in Problem 8.17) states that this property is true in general.

Theorem 8.16: Let λ be any ordinal number. Then $\lambda + 1$ is the immediate successor of A.

General Addition of Ordinal Numbers

Addition of real numbers, which include the natural numbers, is a binary operation and can be extended by induction to any finite sum

$$a_1 + a_2 + \ldots + a_n$$

The sum of an infinite number of real numbers, such as

$$1 + 2 + 3 + 4 + \cdots \quad \text{or} \quad 1 + \tfrac{1}{2} + \tfrac{1}{4} + \cdots$$

has no meaning (unless one introduces the concepts of limits). On the other hand, it is possible to define the sum of an infinite number of ordinal numbers as follows.

Let $\{\lambda_i : i \in I\}$ be any well-ordered collection, finite or infinite, of ordinal numbers. In other words, I is a well-ordered set and to each $i \in I$ there corresponds an ordinal number λ_i. For each $i \in I$, let A_i be a set such that

$$\lambda_i = \text{ord}(A_i)$$

Then the collection of sets $\{A_i \times \{i\} : i \in I\}$ is a well-ordered collection of pairwise disjoint well-ordered sets. By Theorem 8.2,

$$S = \bigcup \{A_i \times \{i\} : i \in I\}$$

is a well-ordered set. Thus the following definition is meaningful.

Definition 8.7: Let $\{\lambda_i : i \in I\}$ be a well-ordered collection of ordinal numbers such that $\lambda_i = \text{ord}(A_i)$. Then

$$\sum_{i \in I} \lambda_i = \text{ord}(\bigcup \{A_i \times \{i\} : i \in I\})$$

According to the above definition, we have

$$1 + 1 + 1 + \cdots = \omega$$

In fact, if each λ_i is finite (and not 0), then

$$\lambda_1 + \lambda_2 + \lambda_3 + \cdots = \sum_{i \in \mathbf{P}} \lambda_i = \omega$$

8.11 ORDINAL MULTIPLICATION

An operation of multiplication is defined for ordinal numbers as follows:

Definition 8.8: Let λ and μ be ordinal numbers and let A and B be well-ordered sets such that $\lambda = \text{ord}(A)$ and $\mu = \text{ord}(B)$. Then

$$\lambda\mu = \text{ord}(A \times B)$$

where $A \times B$ is ordered *reverse lexicographically*.

The product set $A \times B$ is ordered reverse lexicographically means that

$$(a, a') < (b, b') \quad \text{if} \quad \begin{cases} a' < b' \\ \text{or } a' = b' \text{ but } a < b \end{cases}$$

Unless otherwise stated, the product set $A \times B$ of two well-ordered sets A and B is to be ordered reverse lexicographically.

EXAMPLE 8.9 Note first that $2 = \text{ord}(\{a, b\})$ and $\omega = \text{ord}(\{1, 2, 3, \ldots\})$. Then

$$2\omega = \text{ord}(\{(a,1), (b,1), (a,2), (b,2), \ldots\}) = \omega$$

But

$$\omega 2 = \text{ord}(\{(1,a), (2,a), \ldots; (1,b), (2,b), \ldots\}) > \omega$$

since $\mathbf{P} = \{1, 2, 3, \ldots\}$ is similar to the initial segment $\{(1,a), (2,a), \ldots\}$.

The above Example 8.9 tells us that the operation of multiplication of ordinal numbers is not commutative. However, the following conditions do hold.

Theorem 8.17: (1) The associative law for multiplication holds, i.e.,

$$(\lambda\mu)\eta = \lambda(\mu\eta)$$

(2) The left distributive law of multiplication over addition holds; i.e.,

$$\lambda(\mu + \eta) = \lambda\mu + \lambda\eta$$

(3) The ordinal 1 is a multiplicative identity element, i.e.,

$$1\lambda = \lambda 1 = \lambda$$

8.12 STRUCTURE OF ORDINAL NUMBERS

We now write down many of the ordinal numbers according to their order. First come the finite ordinals

$$0,\ 1,\ 2,\ 3,\ \ldots$$

and then comes the first limit ordinal ω and its successors:

$$\omega,\ \omega+1,\ \omega+2,\ \ldots$$

By Example 8.9, $\text{ord}(\{0,1,2,\ldots;\ \omega,\ \omega+1,\omega+2,\ldots\}) = \omega 2$. Hence next comes the second limit ordinal $\omega 2$ and its successors:

$$\omega 2\ ,\omega 2+1,\ \omega 2+2,\ \omega 2+3,\ \ldots$$

The next limit number is $\omega 3$. We proceed as follows:

$$\omega 3,\ \omega 3+1,\ \ldots,\ \omega 4,\ \ldots,\ \omega 5,\ \ldots,\ \ldots,\ \omega\omega = \omega^2$$

Here $\omega\omega = \omega^2$ is the limit number following the limit numbers ωn where $n \in \mathbf{P}$. We continue:

$$\omega^2,\ \omega^2+1,\ \ldots,\ \omega^2+\omega,\ \omega^2+\omega+1,\ \ldots,\ \omega^2+\omega 2,\ \ldots,\ \omega^2+\omega 3,\ \ldots,\ \ldots,\ \omega^2+\omega^2 = \omega^2 2$$

Then

$$\omega^2 2,\ \ldots,\ \omega^2 3,\ \ldots,\ \omega^2 4,\ \ldots,\ \omega^2\omega = \omega^3$$

Then we have the powers of ω:

$$\omega^3,\ \omega^3+1,\ \ldots,\ \omega^4,\ \ldots,\ \omega^5,\ \ldots,\ \ldots,\ \omega^\omega$$

Here ω^ω is the limit number after the limit numbers ω^n where $n \in \mathbf{P}$. We proceed:

$$\omega^\omega,\ \ldots,\ (\omega^\omega)^\omega,\ \ldots,\ ((\omega^\omega)^\omega)^\omega,\ \ldots,\ \ldots$$

After all these ordinals we have the ordinal ϵ_0. We can continue:

$$\epsilon_0,\ \epsilon_0+1,\ \ldots$$

We note that each of the ordinal numbers we have enumerated is still the ordinal number of a countable set.

8.13 AUXILIARY CONSTRUCTION OF ORDINAL NUMBERS

Recall again the following theorem.

Theorem 8.14: Let $s(\lambda)$ be the set of ordinal numbers which precede λ. Then

$$\lambda = \text{ord}(s(\lambda))$$

Some authors use the above property of ordinal numbers to actually define the ordinal numbers. Roughly speaking, an ordinal number is defined to be the set of ordinal numbers which precede it. Specifically:

Definition:

$$0 \equiv \varnothing$$
$$1 \equiv \{0\}$$
$$2 \equiv \{0, 1\}$$
$$3 \equiv \{0, 1, 2\}$$
$$\vdots$$
$$\omega \equiv \{0, 1, 2, \ldots\}$$
$$\omega + 1 \equiv \{0, 1, 2, \ldots, \omega\}$$
$$\omega + 2 \equiv \{0, 1, 2, \ldots, \omega, \omega + 1\}$$
$$\vdots$$
$$\omega 2 \equiv \{0, 1, \ldots, \omega, \omega + 1, \ldots\}$$
$$\omega 2 + 1 \equiv \{0, 1, \ldots, \omega, \omega + 1, \ldots, \omega 2\}$$
$$\vdots$$

One main reason the ordinal numbers are developed as above is in order to avoid certain inherent contradictions which appear in the preceding development of the ordinal numbers (which are discussed in Chapter 9).

Solved Problems

WELL-ORDERED SETS

8.1. Prove Theorem 8.4 (Principle of Transfinite Induction): Let S be a subset of a well-ordered set A with the following properties: (1) $a_0 \in S$, (2) $s(a) \subseteq S$ implies $a \in S$. Then $S = A$.

Suppose $S \neq A$, i.e., suppose $A \backslash S = T$ is not empty. Since A is well-ordered, T has a first element t_0. Each element $x \in s(t_0)$ precedes t_0 and, therefore, cannot belong to T, i.e., belongs to S; hence $s(t_0) \subseteq S$. By (2), $t_0 \in S$. This contradicts the fact that $t_0 \in A \backslash S$. Hence the original assumption that $S \neq A$ is not true; in other words, $S = A$. (Note that (1) is in fact a consequence of (2) since $\varnothing = s(a_0)$ is a subset of S and, therefore, implies $a_0 \in S$.)

8.2. Prove Theorem 8.6: Let $S(A)$ denote the collection of all initial segments of elements in a well-ordered set A, and let $S(A)$ be ordered by set inclusion. Then A is similar to $S(A)$ and, in particular, the function $f: A \to S(A)$ defined by $f(x) = s(x)$ is a similarity mapping between A and $S(A)$.

By definition f is onto. We show that f is one-to-one. Suppose $x \neq y$. Then one of them, say x, strictly precedes the other; hence $x \in s(y)$. But, by definition of initial segment, $x \notin s(x)$. Thus $s(x) \neq s(y)$, and hence f is one-to-one.

We show that f preserves order, that is,

$$x \leq y \quad \text{if and only if} \quad s(x) \subseteq s(y)$$

Let $x \leq y$. Suppose $a \in s(x)$. Then $a \leq x$ and hence $a \leq y$; thus $a \in s(y)$. Since $a \in s(x)$ implies $a \in s(y)$, $s(x)$ is a subset of $s(y)$. Now suppose $x \not\leq y$, that is, $x > y$. Then $y \in s(x)$. But, by definition of initial segment, $y \notin s(y)$; hence $s(x) \not\subseteq s(y)$. In other words, $x \leq y$ if and only if $s(x) \subseteq s(y)$.

8.3. Prove Theorem 8.7: Let A be a well-ordered set, let B be a subset of A, and let $f: A \to B$ be a similarity mapping of A onto B. Then, for every $a \in A$, $a \leq f(a)$.

Let $D = \{x : f(x) < x\}$. If D is empty the theorem is true. Suppose $D \neq \varnothing$. Then, since A is well-ordered, D has a first element d_0. Note $d_0 \in D$ means $f(d_0) < d_0$. Since f is a similarity mapping,

$$f(d_0) < d_0 \qquad \text{implies} \qquad f(f(d_0)) < f(d_0)$$

Consequently, $f(d_0)$ also belongs to D. But $f(d_0) < d_0$ and $f(d_0) \in D$ contradicts the fact that d_0 is the first element of D. Hence the original assumption that $D \neq \varnothing$ leads to a contradiction. Therefore D is empty and the theorem is true.

8.4. Prove Theorem 8.8: Let A and B be similar well-ordered sets. Then there exists only one similarity mapping of A into B.

Let $f: A \to B$ and $g: A \to B$ be similarity mappings. Suppose $f \neq g$. Then there exists an element $x \in A$ such that $f(x) \neq g(x)$. Consequently, either $f(x) < g(x)$ or $g(x) < f(x)$. Say $f(x) < g(x)$. Since $g: A \to B$ is a similarity mapping, $g^{-1}: B \to A$ is also a similarity mapping. Furthermore, $g^{-1} \circ f: A \to A$, the composition of two similarity mappings, is also a similarity mapping. But

$$f(x) < g(x) \qquad \text{implies} \qquad (g^{-1} \circ f)(x) < (g^{-1} \circ g)(x) = x$$

We have $g^{-1} \circ f$ is a similarity mapping and $(g^{-1} \circ f)(x) < x$. This contradicts Theorem 8.7. Hence the assumption that $f \neq g$ leads to a contradiction. Accordingly, there can be only one similarity mapping of A into B.

8.5. Prove Theorem 8.9: A well-ordered set cannot be similar to one of its initial segments.

Let A be a well-ordered set and let $f: A \to s(a)$ be a similarity mapping of A onto one of its initial segments. Then $f(a) \in s(a)$. Therefore

$$f(a) < a$$

This last fact contradicts Theorem 8.7. Therefore A cannot be similar to one of its initial segments.

8.6. Prove: Let A be a well-ordered set and let S be a subset of A with the following property:

$$\text{If } a \leq b \text{ and } b \in S, \text{ then } a \in S.$$

Then $S = A$ or S is an initial segment of A.

Suppose $S \neq A$. Then $A \backslash S$ has a first element a_0 where $a_0 \notin S$. We show that $S = s(a_0)$. Suppose $x \in s(a)$. Then $x < a_0$ and hence $x \notin A \backslash S$. Therefore $x \in S$. Thus $s(a) \subseteq S$.

Now suppose $y \notin s(a_0)$, that is, suppose $a_0 < y$. But $y \in S$ and $a_0 < y$ implies $a_0 \in S$, which contradicts the fact that $a_0 \notin S$. Hence $y \notin S$. We have shown that $y \notin s(a_0)$ implies $y \notin S$, which means that $S \subseteq s(a_0)$.

Both inclusions imply $S = s(a_0)$.

8.7. Prove: Two different initial segments of a well-ordered set cannot be similar.

Let $s(a)$ and $s(b)$ be two different initial segments, that is, $a \neq b$. Either $a < b$ or $b < a$; say $a < b$. Then $s(a)$ is an initial segment of the well-ordered set $s(b)$. Hence, by Theorem 8.9, $s(b)$ is not similar to $s(a)$.

8.8. Prove: Let A and B be well-ordered sets, and let an initial segment $s(a)$ of A be similar to an initial segment of B. Then $s(a)$ is similar to a unique initial segment $s(b)$ of B.

Let $s(a) \simeq s(b)$ and $s(a) \simeq s(b')$ where $b, b' \in B$. Then $s(b) \simeq s(b')$. By Problem 8.7, $s(b) = s(b')$. Therefore, $b = b'$.

8.9. Prove: Let A and B be well-ordered sets such that an initial segment $s(a)$ of A is similar to an initial segment $s(b)$ of B. Then each initial segment of $s(a)$ is similar to an initial segment of $s(b)$, that is,

$$a' \leq a \quad \text{implies} \quad s(a') \simeq s(b') \quad \text{where} \quad b' \leq b$$

Furthermore, if $f: s(a) \to s(b)$ is the similarity mapping of $s(a)$ onto $s(b)$, then f restricted to $s(a')$ is the similarity mapping of $s(a')$ onto $s(b') = f(s(a'))$.

Let $f(a') = b'$. Note that f restricted to $s(a')$ is one-to-one and preserves order; hence $s(a') \simeq f(s(a'))$. Furthermore, since f is a similarity mapping,

$$a^* < a' \quad \text{if and only if} \quad f(a^*) < b'$$

Then $f(s(a')) = s(b')$, and therefore $s(a') \simeq s(b')$.

8.10. Prove: Let A and B be well-ordered sets and let

$$S = \{x : x \in A,\ s(x) \simeq s(y) \text{ where } y \in B\}$$

(In other words, each element $x \in S$ has the property that its initial segment $s(x)$ is similar to an initial segment $s(y)$ of B.) Then $S = A$ or S is an initial segment of A.

Let $x \in S$ and $y < x$. By Problem 8.9, $s(y)$ is similar to an initial segment of B; hence $y \in S$. In other words,

$$y < x \text{ and } x \in S \quad \text{implies} \quad y \in S$$

By Problem 8.6, $S = A$ or S is an initial segment of A.

8.11. Prove: Let A and B be well-ordered sets and let

$$S = \{x : x \in A,\ s(x) \simeq s(y) \text{ where } y \in B\}$$
$$T = \{y : y \in B,\ s(y) \simeq s(x) \text{ where } x \in A\}$$

Then S is similar to T.

Let $x \in S$. Then, by Problem 8.8, $s(x)$ is similar to a unique segment $s(y)$ of B. Thus to each $x \in S$ there corresponds a unique $y \in Y$ such that $s(x) \simeq s(y)$, and vice versa. Hence the function $f: S \to T$ defined by

$$f(x) = y \quad \text{if} \quad s(x) \simeq s(y)$$

is one-to-one and onto.

Now let $x', x \in S, f(x) = y, f(x') = y'$ and $x' < x$. The theorem is proven if we can show that $y' < y$, that is, that f preserves order.

Let $g: s(x) \to s(y)$ be the similarity mapping of $s(x)$ into $s(f(x)) = s(y)$. By Problem 8.9, g restricted to $s(x')$ is a similarity mapping of $s(x')$ into the initial segment $s(g(x'))$ of B. But, by Problem 8.8, there exists only one similarity mapping of $s(x')$ into B. Consequently, $g(x') = f(x') = y'$. Since $g(x') \in s(y)$,

$$g(x') = y' < y$$

Since we have shown that $y' < y$, f preserves order. Therefore, S is similar to T.

8.12. Prove Theorem 8.10: Let A and B be well-ordered sets. Then A is shorter than B, A is similar to B, or A is longer than B.

Let S and T be defined as in the preceding problem. Note $S \simeq T$. By Problem 8.10, there are four possibilities:

Case I: $S = A$ and $T = B$. Then A is similar to B.
Case II: $S = A$ and $T = s(b)$, an initial segment of B. Then A is shorter than B.
Case III: $T = B$ and $S = s(a)$, an initial segment of A. Then A is longer than B.
Case IV: $S = s(a)$ and $T = s(b)$. Then $a \in S$ since its initial segment $s(a)$ is similar to an initial segment $s(b)$ of B. But a cannot belong to its own initial segment; hence this case is impossible.

Thus the theorem is true.

8.13. Prove: Let $\mathscr{A}$ be a collection of initial segments of a well-ordered set A. Then there is an initial segment $s(a) \in \mathscr{A}$ such that $s(a) \subseteq s(x)$ for any other initial segment $s(x)$ in $\mathscr{A}$; that is, there is an initial segment $s(a) \in \mathscr{A}$ which is shorter than every other initial segment in $\mathscr{A}$.

By Theorem 8.6, A is similar to $S(A)$, the family of all initial segments of elements in A, ordered by set inclusion. Since A is well-ordered, $S(A)$ is also well-ordered. Since $\mathscr{A}$ is a subset of $S(A)$, it has a first element $s(a)$. Therefore $s(a) \subseteq s(x)$ for any other initial segment $s(x) \in \mathscr{A}$.

8.14. Prove Theorem 8.11: Let $\mathscr{A}$ be a collection of pairwise nonsimilar well-ordered sets. Then there exists a set A_0 in $\mathscr{A}$ such that A_0 is shorter than every other set in $\mathscr{A}$.

Let B be any set in $\mathscr{A}$. Define

$$\mathscr{B} = \{X : X \in \mathscr{A}, X \text{ is shorter than } B\}$$

If $\mathscr{B}$ is empty, then B satisfies the requirements of the theorem. Suppose $\mathscr{B} \neq \varnothing$. If we show that $\mathscr{B}$ has a shortest set A_0 then, considering the way $\mathscr{B}$ was defined, A_0 will also be the shortest set in $\mathscr{A}$.

Now, by Theorem 8.10, every set $A \in \mathscr{B}$ is similar to an initial segment $s(a)$ of B. Let $\mathscr{B}'$ be the collection of those initial segments of B each of which is similar to a set in $\mathscr{B}$. By Problem 8.13, $\mathscr{B}'$ contains an initial segment $s(a_0)$ which is shorter than every other initial segment in $\mathscr{B}'$. Consequently, the set $A_0 \in \mathscr{B}$, which is similar to $s(a_0)$, is shorter than every other set in $\mathscr{B}$.

Therefore, A_0 satisfies the requirements of the theorem.

ORDINAL NUMBERS

8.15. Prove: Let $\lambda = \text{ord}(A)$ and let $\mu < \lambda$. Then there is a unique initial segment $s(a)$ of A such that $\mu = \text{ord}(s(a))$.

Let $\mu = \text{ord}(B)$. Since $\mu < \lambda$, B is shorter than A, that is, B is similar to an initial segment $s(a)$ of A. Therefore, $\mu = \text{ord}(s(a))$. Furthermore, $s(a)$ is the only initial segment whose ordinal number is μ since, by Problem 8.7, two different initial segments of A cannot be similar.

8.16. Prove Theorem 8.14: Let $s(\lambda)$ be the set of ordinals less than the ordinal λ. Then $\lambda = \text{ord}(s(\lambda))$.

Let $\lambda = \text{ord}(A)$, and let $S(A)$ denote the collection of all initial segments of A ordered by set inclusion. By Theorem 8.5, $A \simeq S(A)$; hence $\lambda = \text{ord}(S(A))$. If we show that $s(\lambda)$ is similar to $S(A)$, the theorem will follow.

Let $\mu \in s(\lambda)$; then $\mu < \lambda$. By Problem 8.15, there is a unique initial segment $s(a)$ of A such that $\mu = \text{ord}(s(a))$. Hence the function $f: s(\lambda) \to S(A)$ defined by

$$f(\mu) = s(a) \qquad \text{if} \qquad \mu = \text{ord}(s(a))$$

is one-to-one. Furthermore, we show that f is onto. Suppose $s(b) \in S(A)$. Then $s(b)$ is shorter than A and therefore $\text{ord}(s(b)) = \nu < \text{ord}(A) = \lambda$. This means $\nu \in s(\lambda)$. Hence $f(\nu) = s(b)$, and so f is onto.

To complete the proof of the theorem, it is only necessary to show that f preserves order; then f is a similarity mapping and $s(\lambda) \simeq S(A)$. Let $\mu < \nu$, where $\mu, \nu \in s(\lambda)$. Then $\mu = \text{ord}(s(a))$ and $\nu = \text{ord}(s(b))$, that is, $f(\mu) = s(a)$ and $f(\nu) = s(b)$. Since $\mu < \nu$, $s(a)$ is an initial segment of $s(b)$; hence $s(a)$ is a proper subset of $s(b)$. In other words, under the ordering of $S(A)$, $s(a) < s(b)$. Thus f preserves order.

8.17. Prove Theorem 8.16: Let λ be any ordinal number. Then $\lambda + 1$ is the immediate successor of λ.

Let μ be the immediate successor of λ. Then, by definition of $s(\mu)$,

$$s(\mu) = s(\lambda) \cup \{\lambda\}$$

Hence

$$\text{ord}(s(\mu)) = \text{ord}(s(\lambda)) + \text{ord}(\{\lambda\})$$

That is, $\mu = \lambda + 1$.

8.18. Prove, by giving a counterexample, that the right distributive law of multiplication over addition (for the ordinal numbers) is not true in general. In other words, exhibit three ordinal numbers λ, μ, ν such that

$$(\lambda + \mu)\nu \neq \lambda\nu + \mu\nu$$

By Example 8.9, $(1 + 1)\omega = 2\omega = \omega$. On the other hand, using the left distributive law,

$$1\omega + 1\omega = \omega + \omega = \omega 1 + \omega 1 = \omega(1 + 1) = \omega 2 > \omega$$

Therefore, $(1 + 1)\omega \neq 1\omega + 1\omega$.

8.19. Let $\{A_i : i \in I\}$ be a well-ordered collection of pairwise disjoint well-ordered sets. Suppose $\text{ord}(I) = \omega$ and $\text{ord}(A_i) = \omega$ for every $i \in I$. Find $\text{ord}(\bigcup_i A_i)$.

$$\text{ord}(\textstyle\bigcup_i A_i) = \omega\omega + \omega + \cdots = \omega(1 + 1 + 1 + \cdots) = \omega\omega = \omega^2$$

8.20. Prove: $\omega + \omega = \omega 2$.

Method 1: Using the left distributive law we get

$$\omega + \omega = \omega 1 + \omega 1 = \omega(1 + 1) = \omega 2$$

Method 2: Consider the well-ordered sets

$$A = \{a_1, a_2, \ldots\}, \qquad B = \{b_1, b_2, \ldots\}, \qquad C = \{c_1, c_2, \ldots\}, \qquad D = \{r, s\}$$

Note that

$$\omega = \text{ord}(A) = \text{ord}(B) = \text{ord}(C) \qquad \text{and} \qquad 2 = \text{ord}(D)$$

Then

$$\omega + \omega = \text{ord}(\{A; B\}) = \text{ord}(\{a_1, a_2, \ldots; b_1, b_2, \ldots\})$$
$$\omega 2 = \text{ord}(C \times D) = \text{ord}(\{(c_1, r), (c_2, r), \ldots; (c_1, s), (c_2, s), \ldots\})$$

But the function f: $\{A; B\} \to \{C \times D\}$ defined by

$$f(x) = \begin{cases} (c_i, r) & \text{if } x = a_i \\ (c_i, s) & \text{if } x = b_i \end{cases}$$

is a similarity mapping of $\{A; B\}$ onto $C \times D$. Hence

$$\omega + \omega = \text{ord}(\{A; B\}) = \text{ord}(\{C \times D\}) = \omega 2$$

Supplementary Problems

8.21. Prove Theorem 8.1: Let A be a well-ordered set. Then: (i) Every subset of A is well-ordered. (ii) If B is similar to A, then B is well-ordered

8.22. Prove Theorem 8.2: Let $\{A_i : i \in I\}$ be a well-ordered family of pairwise disjoint well-ordered sets. Then the union $S = \bigcup_i A_i$ (with the usual ordering) is well-ordered.

8.23. Assume that the set $\mathbf{P}$ of counting numbers with the usual order is well-ordered. Prove the Principle of Mathematical Induction: Let S be a subset of $\mathbf{P}$ with the properties:

$$(1)\ 1 \in S \text{ and } (2)\ n \in S \text{ implies } n+1 \in S;$$

then $S = \mathbf{P}$.

8.24. Prove that 0 is the identity element for addition of ordinal numbers, that is, for any ordinal λ, we have $0 + \lambda = \lambda + 0 = \lambda$.

8.25. Prove that 1 is the identity element for multiplication of ordinal numbers, that is, for any ordinal λ, we have $1\lambda = \lambda 1 = \lambda$.

8.26. Prove: If each λ_i, $i \in \mathbf{P}$, is a finite ordinal, then $\lambda_1 + \lambda_2 + \cdots = \sum_i \lambda_i = \omega$.

8.27. Prove: Let λ be any infinite ordinal number. Then $\lambda = \mu + n$, where μ is a limit number and n is a finite ordinal.

8.28. State whether each of the following statements about ordinals is true or false; if it is true prove it, and if it is false give a counterexample: (*a*) If $\lambda \neq 0$, then $\mu < \lambda + \mu$. (*b*) If $\lambda \neq 0$, then $\mu < \mu + \lambda$.

8.29. State whether each of the following statements concerning ordinals is true or false; if it is true prove it, and if it is false give a counterexample:

(*a*) If $\lambda \neq 0$ and $\mu < \nu$, then $\lambda + \mu < \lambda + \nu$.

(*b*) If $\lambda \neq 0$ and $\mu < \nu$, then $\mu + \lambda < \nu + \lambda$.

8.30. Prove: The left distributive law of multiplication over addition holds for ordinal numbers, that is,

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu$$

Answers to Supplementary Problems

8.27. *Hint*: Note that a well-ordered set cannot contain an ordered subset $A = \{\cdots < a_3 < a_2 < a_1\}$, since A is not well-ordered.

8.28. (*a*) False. (*b*) True

8.29. (*a*) True. (*b*) False

Chapter 9

Axiom of Choice, Zorn's Lemma, Well-Ordering Theorem

9.1 INTRODUCTION

Many properties of well-ordered sets were investigated in the preceding Chapter 8. We have not said much about the existence of such sets. Central to the theory of set theory is the fact that any set can be well-ordered! This was proved by E. Zermelo in 1904. Specifically, this "well-ordering theorem" can be shown to be equivalent to the axiom of choice and Zorn's lemma. This equivalence and some of its consequences will be treated in this chapter. We will end the chapter with some paradoxes in set theory.

9.2 CARTESIAN PRODUCTS AND CHOICE FUNCTIONS

The following theorem applies.

Definition 9.1: Let $\{A_i : i \in I\}$ be a nonempty family of nonempty sets. Then the cartesian product of $\{A_i : i \in I\}$, denoted by

$$\prod\{A_i : i \in I\} \text{ or } \prod_i A_i$$

is the set of all choice functions defined on $\{A_i : i \in I\}$.

Recall that a function f: $\{A_i : i \in I\} \to X$, where each A_i is a subset of X, is called a choice function if $f(A_i) = a_i$ belongs to A_i, for every $i \in I$. In other words, f "chooses" a point $a_i \in A_i$ for each set A_i.

EXAMPLE 9.1 Let $\{A_1, A_2, \ldots, A_n\}$ be a finite family of sets. Recall (Chapter 2) that the cartesian product of the n sets,

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i$$

is defined to be the set of n-tuples

$$(a_1, a_2, \ldots, a_n)$$

where $a_i \in A_i$ for $i = 1, 2, \ldots, n$. On the other hand, each choice function f defined on $\{A_1, A_2, \ldots, A_n\}$ corresponds to the unique n-tuple

$$(f(A_1), f(A_2), \ldots, f(A_n))$$

and vice versa. Accordingly, in the finite case, Definition 9.1 agrees with the previous definition of the cartesian product.

The main reason for introducing Definition 9.1 is that it applies to any family of sets: finite, denumerable, or even nondenumerable. The previous definition, which used the concept of n-tuples, applied only to a finite family of sets.

Remark: Although a choice function is defined for a family of subsets, any family of sets $\{A_i : i \in I\}$ can be considered to be a family of subsets of their union $\bigcup_i A_i$.

9.3 AXIOM OF CHOICE

The axiom of choice lies at the foundations of mathematics and, in particular, the theory of sets. This "innocent looking" axiom, which follows, has as a consequence some of the most powerful and important results in mathematics.

Axiom of Choice: The cartesian product of a nonempty family of nonempty sets is nonempty.

Using Definition 9.1, the axiom of choice can be stated as follows:

Axiom of Choice: There exists a choice function for any nonempty family of nonempty sets.

The axiom of choice is equivalent to the following postulate:

Zermelo's Postulate: Let $\{A_i : i \in I\}$ be any nonempty family of disjoint nonempty sets. Then there exists a subset B of the union $\bigcup_i A_i$ such that the intersection of B and each set A_i consists of exactly one element.

Observe that in Zermelo's postulate the sets are disjoint whereas in the axiom of choice they may not be disjoint.

9.4 WELL-ORDERING THEOREM, ZORN'S LEMMA

The following theorem is attributed to Zermelo, who proved the theorem directly from the axiom of choice.

Well-Ordering Theorem: Every set can be well-ordered.

Zorn's lemma, which follows, is one of the most important tools in mathematics; it establishes the existence of certain types of elements although no constructive process is given to find these elements.

Zorn's Lemma: Let X be a nonempty partially ordered set in which every chain (linearly ordered subset) has an upper bound in X. Then X contains at least one maximal element.

We formally state and prove (Problem 9.4) the following basic result of set theory:

Theorem 9.1: The following are equivalent:

(i) Axiom of choice;
(ii) Well-ordering theorem;
(iii) Zorn's lemma.

9.5 CARDINAL AND ORDINAL NUMBERS

Let $\lambda = \text{ord}(A)$ be an ordinal number. Then we can associate with λ the unique cardinal number $\alpha = |A|$. We call α the cardinal number of λ and denote it by

$$\alpha = \overline{\lambda}$$

This function from the ordinal numbers to the cardinal numbers is not one-to-one, that is, there are different ordinal numbers with the same cardinal number. For example,

$$\omega = \text{ord}(\{1, 2, 3, \ldots\}) \quad \text{and} \quad \omega 2 = \text{ord}(\{a_1, a_2, \ldots; b_1, b_2, \ldots\})$$

are both ordinal numbers of denumerable sets with the same cardinal number $\aleph_0$. In other words,

$$\overline{\omega} = \aleph_0 = \overline{\omega 2}$$

The well-ordering theorem implies that the above function from the ordinal numbers to the cardinal

numbers is onto. For, suppose $\alpha = |A|$ is any cardinal number. By the well-ordering theorem, A can be well-ordered; say $\lambda = \text{ord}(A)$. Then $\alpha = \overline{\lambda}$. Hence α is the cardinal number of at least one ordinal number λ. (Here, A is used both as the original set and then as the well-ordered set.)

Correspondence between Ordinal and Cardinal Numbers

The following correspondence between the ordinal and cardinal numbers is easily established.

Theorem 9.2: Let $\alpha = \overline{\lambda}$ and $\beta = \overline{\mu}$ be cardinal numbers. Then:

(1) If $\alpha < \beta$, then $\lambda < \mu$.

(2) If $\lambda < \mu$, then $\alpha \leq \beta$.

The next result, mentioned previously, is a direct consequence of the well-ordering theorem.

Theorem 6.12 (Law of Trichotomy): Let α and β be any cardinal numbers. Then one of the following holds:

$$\alpha < \beta, \qquad \alpha = \beta, \qquad \alpha > \beta$$

That is, the cardinal numbers are linearly ordered by the inequality relation defined for the cardinal numbers. Since the ordinal numbers are themselves well-ordered, we can make an even stronger statement.

Theorem 9.3: Any set of cardinal numbers is well-ordered by the relation $\alpha \leq \beta$.

9.6 ALEPHS

Recall that the cardinal number of denumerable sets is denoted by

$$\aleph_0$$

(Here aleph, $\aleph$, is the first letter of the Hebrew alphabet.) Since the cardinal numbers are well-ordered, the following system of notation is used to denote cardinal numbers. The immediate successor of $\aleph_0$ is denoted by $\aleph_1$, and its immediate successor by $\aleph_2$, and so on. The cardinal number which succeeds all the $\aleph_n$ is denoted by $\aleph_\omega$. In fact every infinite cardinal can be uniquely denoted by an $\aleph$ with an ordinal number as a subscript as follows:

Notation: Let α be any infinite cardinal number. Let $s(\alpha)$ be the set of infinite cardinal numbers less than α. Note that $s(\alpha)$ is well-ordered; say $\lambda = \text{ord}(s(\alpha))$. Then

$$\aleph_\lambda$$

denotes the cardinal number α.

The continuum hypothesis can now be reformulated as follows:

Continuum Hypothesis: $\aleph_1 = \mathfrak{c}$.

9.7 PARADOXES IN SET THEORY

The theory of sets was first studied as a mathematical discipline by Cantor (1845–1918) in the latter part of the nineteenth century. Today, the theory of sets lies at the foundations of mathematics and has revolutionized almost every branch of mathematics. At about the same time that set theory began to influence other branches of mathematics, various contradictions, called paradoxes, were discovered, the first by Burali-Forti in 1897. In this section, some of these paradoxes are presented. Although it is possible to eliminate these known contradictions by a strict axiomatic development of set theory, there are still many questions which are unanswered.

Set of All Sets (Cantor's Paradox)

Let $\mathscr{C}$ be the set of all sets. Then every subset of $\mathscr{C}$ is also a member of $\mathscr{C}$; hence the power set $\mathscr{P}(\mathscr{C})$ of $\mathscr{C}$ is a subset of $\mathscr{C}$, that is,

$$\mathscr{P}(\mathscr{C}) \subseteq \mathscr{C}$$

But $\mathscr{P}(\mathscr{C}) \subseteq \mathscr{C}$ implies that

$$|\mathscr{P}(\mathscr{C})| \leq |\mathscr{C}|$$

However, according to Cantor's theorem,

$$|\mathscr{C}| < |\mathscr{P}(\mathscr{C})|$$

Thus the concept of the set of all sets leads to a contradiction.

Russell's Paradox

Let Z be the collection of all sets which do not contain themselves as members, that is,

$$Z = \{X : X \notin X\}$$

Question: Does Z belong to itself or not?

If Z does not belong to Z then, by definition of Z, the set Z does belong to itself. On the other hand, if Z does belong to Z then, by definition of Z, the set Z does not belong to itself. In either case we are led to a contradiction.

The above paradox is somewhat analogous to the following popular paradox: In a certain town, there is a barber who shaves only and all those men who do not shave themselves. Question: Who shaves the barber?

Set of All Ordinal Numbers (Burali-Forti Paradox)

Let Δ be the set of all ordinal numbers. By a previous theorem Δ is a well-ordered set, say $\alpha = \text{ord}(\Delta)$. Now consider $s(\alpha)$, the set of all ordinal numbers less than α. Note:

(1) Since $s(\alpha)$ consists of all elements in Δ which precede α, $s(\alpha)$ is an initial segment of Δ.
(2) By a previous theorem $\alpha = \text{ord}(s(\alpha))$; hence $\text{ord}(s(\alpha)) = \alpha = \text{ord}(\Delta)$.

Therefore Δ is similar to one of its initial segments, which is not possible. Thus the concept of the set of all ordinal numbers leads to a contradiction of Theorem 8.9.

Set of All Cardinal Numbers

Let $\mathscr{A}$ be the set of all cardinal numbers. Then for each cardinal $\alpha \in \mathscr{A}$ there is a set A_α such that $\alpha = |A_\alpha|$. Let

$$A = \bigcup(A_\alpha : \alpha \in \mathscr{A})$$

Consider the power set $\mathscr{P}(A)$ of A. Note $\mathscr{P}(A) \approx A_{|\mathscr{P}(A)|}$, which is a subset of A. Hence

$$|\mathscr{P}(A)| \leq |A|$$

But by Cantor's theorem,

$$|A| < |\mathscr{P}(A)|$$

Thus the concept of the set of all cardinal numbers leads to a contradiction.

Class of All Sets Equipotent to a Set

Let $A = \{a, b, \ldots\}$ be any set (not necessarily countable) and let $\mathscr{A} = \{i, j, \ldots\}$ be any other set. Consider the sets

$$A_i = \{(a, i), (b, i), \ldots\}$$
$$A_j = \{(a, j), (b, j), \ldots\}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

that is, the class of sets $\{A_i : i \in \mathscr{A}\}$. Note that

$$|\{A_i : i \in \mathscr{A}\}| = |\mathscr{A}|$$

and $A_i \approx A$ for every $i \in \mathscr{A}$.

Now let α be the class of all sets equipotent to A. Consider the power set $\mathscr{P}(\alpha)$ of α, and define the class of sets $\{A_i : i \in \mathscr{P}(\alpha)\}$ as above. Since each $A_i \approx A$, we have

$$\{A_i : i \in \mathscr{P}(\alpha)\} \subseteq \alpha$$

Hence

$$|\mathscr{P}(\alpha)| = |\{A_i : i \in \mathscr{P}(\alpha)\}| \leq |\alpha|$$

But by Cantor's theorem, $|\alpha| < |\mathscr{P}(\alpha)|$. Thus the concept of the class of all sets equipotent to a set leads to a contradiction.

Class of All Sets Similar to a Well-Ordered Set

Let A be any well-ordered set. Then the set A_i, defined as above and ordered by

$$(a, i) \leq (b, i) \quad \text{if} \quad a \leq b$$

is well-ordered and is similar to A, that is, $A_i \simeq A$.

Now let λ be the class of all sets similar to the well-ordered set A. Consider the power set $\mathscr{P}(\lambda)$ of λ and define the class of sets $\{A_i : i \in \mathscr{P}(\lambda)\}$ as above. Since each set A_i is similar to A, we have

$$\{A_i : i \in \mathscr{P}(\lambda)\} \subseteq \lambda$$

Hence

$$|\mathscr{P}(\lambda)| = |\{A_i : i \in \mathscr{P}(\lambda)\}| \leq |\lambda|$$

But by Cantor's theorem, $|\lambda| < |\mathscr{P}(\lambda)|$. Thus the concept of the class of all sets similar to a well-ordered set leads to a contradiction.

Solved Problems

AXIOM OF CHOICE

9.1. Show that the axiom of choice is equivalent to Zermelo's postulate.

Let $\{A_i : i \in I\}$ be a nonempty family of disjoint nonempty sets and let f be a choice function on $\{A_i : i \in I\}$. Set $B = \{f(A_i) : i \in I\}$. Then

$$A_i \cap B = \{f(A_i)\}$$

consists of exactly one element since the A_i are disjoint and f is a choice function. Accordingly, the axiom of choice implies Zermelo's postulate.

Now let $\{A_i : i \in I\}$ be any nonempty family of nonempty sets which may or may not be disjoint. Set

$$A_i^* = \{A_i\} \times \{i\} \qquad \text{for every } i \in I$$

Then certainly $\{A_i^*\}$ is a disjoint family of sets since $i \neq j$ implies $A_i \times \{i\} \neq A_j \times \{j\}$, even if $A_i = A_j$. By Zermelo's postulate, there exists a subset B of $\bigcup\{A_i^* : i \in I\}$ such that

$$B \cap A_i^* = \{(a_i, i)\}$$

consists of exactly one element. Then $a_i \in A_i$, and so the function f on $\{A_i : i \in I\}$ defined by $f(A_i) = a_i$ is a choice function. Accordingly, Zermelo's postulate implies the axiom of choice.

9.2. Prove the well-ordering theorem (Zermelo): Every nonempty set X can be well-ordered.

Let f be a choice function on the collection $\mathscr{P}(X)$ of all subsets of X, that is,

$$f: \mathscr{P}(X) \to X \qquad \text{with} \qquad f(A) \in A, \qquad \text{for} \qquad \text{every } A \subseteq X$$

A subset A of X will be called *normal* if it has a well-ordering with the additional property that, for every $a \in A$,

$$f(X - s_A(a)) = a \qquad \text{where} \qquad s_A(a) = \{x \in A : x < a\}$$

i.e., $s_A(a)$ is the initial segment of a in the ordering of A. We show that normal sets exist. Set

$$x_0 = f(X), \qquad x_1 = f(X \backslash \{x_0\}), \qquad x_2 = f(X \backslash \{x_0, x_1\})$$

Then $A = \{x_0, x_1, x_2\}$ is normal. We claim that if A and B are normal subsets of X, then either $A = B$ or one is an initial segment of the other. Since A and B are well-ordered, one of them, say A, is similar to B or to an initial segment of B (Theorem 8.10). Thus there exists a similarity mapping $\alpha : A \to B$. Set

$$A^* = \{x \in A : \alpha(x) \neq x\}$$

If A^* is empty, then $A = B$ or A is an initial segment of B. Suppose $A^* \neq \varnothing$, and let a_0 be the first element of A^*. Then $s_A(a_0) = s_B(\alpha(a_0))$. But A and B are normal, and so

$$a_0 = f(X) \backslash s_A(a_0)) = f(X \backslash s_B(\alpha(a_0))) = \alpha(a_0)$$

But this contradicts the definition of A^*, and so $A = B$ or A is an initial segment of B. In particular, if $a \in A$ and $b \in B$ then either $a, b \in A$ or $a, b \in B$. Furthermore, if $a, b \in A$ and $a, b \in B$ then $a \leq b$ as elements of A if and only if $a \leq b$ as elements of B.

Now let Y consist of all those elements in X which belong to at least one normal set. If $a, b \in Y$, then $a \in A$ and $b \in B$ where A and B are normal and so, as noted above, $a, b \in A$ or $a, b \in B$. We define an order in Y as follows: $a \leq b$ as elements of Y iff $a \leq b$ as elements of A or as elements of B. This order is well-defined, i.e., independent of the particular choice of A and B, and, furthermore, it is a linear order. Now let Z be any nonempty subset of Y and let a be any arbitrary element in Z. Then a belongs to a normal set A. Hence $A \cap Z$ is a nonempty subset of the well-ordered set A and so contains a first element a_0. Furthermore, a_0 is a first element of Z (Problem 9.13); thus Y is, in fact, well-ordered.

We next show that Y is normal. If $a \in Y$, then a belongs to a normal set A. Furthermore, $s_A(a) = s_Y(a)$ (Problem 9.13), and so

$$f(X \backslash s_Y(a)) = f(X \backslash s_A(a)) = a$$

that is, Y is normal. Lastly, we claim that $Y = X$. Suppose not, i.e., suppose $X \backslash Y \neq \varnothing$ and, say, $a = f(X \backslash Y)$. Set $Y^* = Y \cup \{a\}$ and let Y^* be ordered by the order in Y together with a dominating every element in Y. Then $f(X \backslash s_Y(a)) = f(X \backslash Y) = a$ and so Y^* is normal. Thus $a \in Y$. But this contradicts the fact that f is a choice function, i.e., $f(X \backslash Y) = a \in X \backslash Y$ which is disjoint from Y. Hence $Y = X$, and so X is well-ordered.

9.3. Prove (using the well-ordering theorem): Let X be a partially ordered set. Then X contains a maximal chain (linearly ordered subset), i.e., a chain which is not a proper subset of any other chain.

The result clearly holds if X is empty (or even finite); hence we can assume that X is not empty and that X can be well-ordered with, say, first element x_0. (Observe that X now has both a partial ordering and a well-ordering; the terms initial segment of X and first element of a subset of X will only be used with respect to the well-ordering, and the term comparable will only be used with respect to the partial ordering.)

Let A be an initial segment of X (where we allow $A = X$). A function $f: A \to A$ will be called *special* if

$$f(x) = \begin{cases} x, & \text{if } x \text{ is comparable to every element of } f[s(x)] \\ x_0, & \text{otherwise.} \end{cases}$$

Here $s(x)$ denotes the initial segment of x. We claim that if a special function exists then it is unique. If not, then there exist special functions f and f' on A and a first element a_0 for which $f(a_0) \neq f'(a_0)$; hence f and f' agree on $s(a_0)$, which implies $f(a_0) = f'(a_0)$, a contradiction.

Remark: If A and A' are initial segments with special functions f and f' respectively and if $A \subseteq A'$, then the uniqueness of f on A implies that f' restricted to A equals f, i.e., $f'(a) = f(a)$ for every $a \in A$.

Now let B be the union of those A_i which admit a special function f_i. Since the A_i are initial segments, so is B. Furthermore, B admits the special function $g: B \to B$ defined by $g(b) = f_i(b)$ where $b \in A_i$. By the above remark, g is well-defined. We next show that $B = X$. Let $y \in X$ be the first element for which $y \notin B$. Then $C = B \cup \{y\}$ is an initial segment. Moreover, C admits the special function $h: C \to C$ defined as follows: $h(c) = g(c)$ if $c \in B$, and $h(y) = y$ or x_0 according as y is or is not comparable to every element in $h[B]$. It now follows that $y \in B$, a contradiction. Thus no such y exists and so $B = X$.

Lastly, we claim that $g[B]$, i.e., $g[X]$, is a maximal chain (linearly ordered subset) of X. If not, then there exists an element $z \in X$ such that $z \notin g[X]$ but z is comparable to every element of $g[X]$. Thus, in particular, z is comparable to every element of $g[s(z)]$. By definition of a special function, $g(z) = z$ which implies $z \in g[X]$, a contradiction. Thus $g[X]$ is a maximal chain of X, and the theorem is proved.

9.4. Prove Theorem 9.1: The following are equivalent: (i) axiom of choice, (ii) well-ordering theorem, (iii) Zorn's lemma.

By Problem 9.2, (i) implies (ii). We use Problem 9.3 to prove that (ii) implies (iii). Let X be a partially ordered set in which every chain (linearly ordered subset) has an upper bound. We need to show that X has a maximal element. By Problem 9.3, X has a maximal chain, say Y. By hypothesis, Y has an upper bound m in X. We claim that m is a maximal element of X. If not, then there exists $z \in X$ such that z dominates m. It follows that $z \notin Y$ since m is an upper bound for Y, and that $Y \cup \{z\}$ is linearly ordered. This contradicts the maximality of Y. Thus m is a maximal element of X and, consequently, (ii) implies (iii).

It remains to show that (iii) implies (i). By Problem 9.1, it suffices to prove that (iii) implies Zermelo's postulate. Let $\{A_i\}$ be a nonempty family of disjoint nonempty sets. Let $\mathscr{B}$ be the class of all subsets of $\bigcup_i A_i$ which intersect each A_i in at most one element. We partially order $\mathscr{B}$ by set inclusion. Let $\mathscr{C} = \{B_j\}$ be a chain of $\mathscr{B}$. We claim that $B = \bigcup_j B_j$ belongs to $\mathscr{B}$. If not, then B intersects some A_{i_0} in more than one element; say $a, b \in B \cap A_{i_0}$ where $a \neq b$. Since $a, b \in B$, there exist B_{j_1} and B_{j_2} such that $a \in B_{j_1}$ and $b \in B_{j_2}$. But $\mathscr{C} = \{B_j\}$ is linearly ordered by set inclusion; hence a and b belong to either B_{j_1} or B_{j_2}. This implies that B_{j_1} or B_{j_2} intersects A_{i_0} in more than one element, a contradiction. Accordingly, B belongs to $\mathscr{B}$, and so B is an upper bound for the chain $\mathscr{C}$.

We have shown that every chain in $\mathscr{B}$ has an upper bound. By Zorn's lemma, $\mathscr{B}$ has a maximal element M. If M does not intersect each A_i in exactly one point, then M and some A_{i_k} are disjoint. Say $c \in A_{i_k}$. Then $M \cup \{c\}$ belongs to $\mathscr{B}$, which contradicts the maximality of M. Thus M intersects each A_i in exactly one point, and therefore (iii) implies Zermelo's postulate.

Thus the theorem is proved.

APPLICATIONS OF ZORN'S LEMMA

9.5. Let R be a relation from A to B, that is, let R be a subset of $A \times B$. Suppose the domain of R is A. Prove that there exists a subset f^* of R such that f^* is a function from A into B.

Let $\mathscr{A}$ be the family of subsets of R in which each $f \in \mathscr{A}$ is a function from a subset of A into B. Partially order $\mathscr{A}$ by set inclusion. Note that if $f: A_1 \to B$ is a subset of $g: A_2 \to B$ then $A_1 \subseteq A_2$.

Now suppose $\mathscr{C} = \{f_i : A_i \to B\}$ is a chain (linearly ordered subset) of $\mathscr{A}$. Then (Problem 9.14) $f = \bigcup_i f_i$ is a function from $\bigcup_i A_i$ into B and, therefore, f is an upper bound of $\mathscr{C}$. By Zorn's lemma, $\mathscr{A}$ has a maximal element $f^*: A^* \to B$. If we show that $A^* = A$, then the theorem is proved.

Suppose $A^* \neq A$. Then there exists an element $a \in A$ such that $a \notin A^*$. Furthermore, since the domain of R is A, there exists an ordered pair $(a, b) \in R$. Then $f^* \cup \{(a, b)\}$ is a function from $A^* \cup \{a\}$ into B. But this contradicts the fact that f^*, which would be a proper subset of $f^* \cup \{(a, b)\}$, is a maximal element of $\mathscr{A}$. Therefore $A^* = A$, and the theorem is proved.

9.6. (Application to Linear Algebra.) Prove that every vector space V has a basis.

If V consists of the zero vector alone then, by definition, the empty set is a basis for V; hence we assume V contains a nonzero vector a. Let $\mathscr{B}$ be the family of independent sets of vectors in V. In other words, each element $B \in \mathscr{B}$ is an independent set of vectors. Note that $\mathscr{B}$ is nonempty since, e.g., $\{a\}$ belongs to $\mathscr{B}$. Partial order $\mathscr{B}$ by set inclusion.

Now suppose $\mathscr{C} = \{B_i\}$ is a chain of $\mathscr{B}$. If we show that $A = \bigcup_i B_i$ belongs to $\mathscr{B}$, i.e., A is an independent set of vectors, then A would be an upper bound of $\mathscr{C}$. Assume that A is dependent. Then there exist vectors $a_1, a_2, \ldots, a_n$ in A and scalars $c_1, c_2, \ldots, c_n$, not all zero, such that

$$c_1 a_1 + c_2 a_2 + \cdots + c_n a_n = 0 \tag{1}$$

Since each $a_j \in A$, there exists $B_{j'}$ in $\mathscr{C}$ such that $a_j \in B_{j'}$. Since $\mathscr{C} = \{B_i\}$ is linearly ordered, one of the sets $B_{1'}, B_{2'}, \ldots B_{n'}$, say $B_{1'}$, is a superset of the others; hence $a_1, a_2, \ldots, a_n$ all belong to $B_{1'}$. In view of (1), $B_{1'}$ would be dependent, which is a contradiction. Thus A is independent, A belongs to $\mathscr{B}$, and A is an upper bound of $\mathscr{C}$.

By Zorn's lemma, $\mathscr{B}$ has an upper bound B^*. B^* can then be shown to be a basis for V.

Remark: The main part of the proof consists in showing that $A = \bigcup_i B_i$ does belong to $\mathscr{B}$. This is a typical example of how Zorn's lemma is used.

9.7. (Application to Algebra.) Let R be a ring with unity 1. Prove that every proper ideal J of R is contained in a maximal ideal.

Recall that an ideal J is proper if $J \neq R$, and an ideal M is maximal if no ideal K properly lies between M and R, that is, if $M \subseteq K \subseteq R$, then $M = K$ or $K = R$. Also, when R has a unity element 1, an ideal J is proper if and only if $1 \notin J$.

Let J be any proper ideal of R. Let $\mathscr{A}$ be the collection of all proper ideals of R which contain J. $\mathscr{A}$ is not empty since $J \in \mathscr{A}$. Partially order $\mathscr{A}$ by set inclusion. Suppose $\mathscr{C}$ is a chain in $\mathscr{A}$. Let M be the union of the ideals in $\mathscr{C}$. Now M is an ideal since the union of an ascending chain of ideals is an ideal. Since 1 is not in any ideal of $\mathscr{C}$, $1 \notin M$ and hence M is a proper ideal. Thus $M \in \mathscr{A}$. Clearly, M is an upper bound for $\mathscr{C}$. By Zorn's lemma, $\mathscr{A}$ has a maximal element J^*. Then J^* is a maximal ideal containing J.

Supplementary Problems

9.8. State whether each of the following statements about cardinal numbers is true or false and give reasons for your answer:

(*a*) $\aleph_0 + \aleph_\lambda = \aleph_\lambda$; (*b*) $\aleph_\lambda + \aleph_\mu = \aleph_{\lambda+\mu}$.

9.9. Prove Theorem 9.2: Let $\alpha = \overline{\lambda}$ and $\beta = \overline{\mu}$ be cardinal numbers. Then:

(i) $\alpha < \beta$ implies $\lambda \preccurlyeq \mu$; (ii) $\lambda < \mu$ implies $\alpha \leq \beta$.

9.10. Prove Theorem 6.12 (Law of Trichotomy). For any cardinal numbers α and β, exactly one of the following holds:

$$\alpha < \beta, \quad \alpha = \beta, \quad \alpha > \beta.$$

9.11. Prove Theorem 9.3: Any set of cardinal numbers is well-ordered by the relation $\alpha \leq \beta$.

9.12. Consider the proof of the following statement:

There exists a finite set of natural numbers which is not a proper subset of another finite set of natural numbers.

Proof: Let $\mathscr{B}$ be the family of all finite sets of natural numbers. Partially order $\mathscr{B}$ by set inclusion. Now let $\mathscr{C} = \{B_i\}$ be a chain of $\mathscr{B}$. Let $A = \bigcup_i B_i$. Note that each $B_i \subseteq A$. Hence A is an upper bound of $\mathscr{C} = \{B_i\}$. Thus every chain of $\mathscr{B}$ has an upper bound. By Zorn's lemma, $\mathscr{B}$ has a maximal element, a finite set which is not a proper subset of another finite set.

Question: Since the statement is obviously false, which step in the proof is incorrect?

9.13. Prove the following two statements which were assumed in the proof in Problem 9.2:

(i) The first element a_0 of the set $A \cap Z$ is a first element of the set Z.

(ii) $s_A(a) = s_Y(a)$.

9.14. Prove the following statement which was assumed in the proof in Problem 9.5: Let $\{f_i : A_i \to B\}$ be a collection of functions which is linearly ordered by set inclusion. Then $\bigcup_i f_i$ is a function from $\bigcup_i A_i$ into B.

Answers to Supplementary Problems

9.8. (*a*) True. For $\aleph_0$ is the cardinal number of a denumerable set and, as proven previously, the union of a denumerable set and an infinite set does not change the cardinality of the infinite set.

(*b*) False. If not, since the addition of cardinals is commutative, we would have

$$\aleph_{\lambda+\mu} = \aleph_\lambda + \aleph_\mu = \aleph_\mu + \aleph_\lambda = \aleph_{\mu+\lambda}$$

This would imply that the addition of ordinal numbers is commutative, which is not true.

9.12. A does not belong to $\mathscr{C} = \{B_i\}$.